Scientia et Ratio
ISSN 2525-8532

A EVOLUÇÃO DO CONCEITO DE CRIME CIBERNÉTICO NO ORDENAMENTO JURÍDICO BRASILEIRO: O PARADOXO ENTRE INOVAÇÃO E TAXATIVIDADE PENAL

THE EVOLUTION OF THE CONCEPT OF CYBERCRIME IN THE BRAZILIAN LEGAL SYSTEM: THE PARADOX BETWEEN INNOVATION AND CRIMINAL TAXATIVITY

Artigo submetido em 23 de maio de 2026
Artigo aprovado em 25 de maio de 2026
Artigo publicado em 25 de maio de 2026

Scientia et Ratio
Volume 6 – Número 10 – 2026
ISSN 2525-8532

.

Autor:
Karolline Ribeiro Bentes[1]
Igor Câmara de Araújo [2]

.

RESUMO: Este artigo analisa a evolução legislativa dos crimes cibernéticos no Brasil, confrontando-a com os princípios da Anterioridade e da Taxatividade Penal. Nosso problema de pesquisa questiona se a legislação atual consegue acompanhar a velocidade das

inovações ou se o Estado tem criado apenas leis de ocasião. O objetivo é mapear essa trajetória, desde o vácuo normativo até as recentes tipificações, definindo os delitos próprios e impróprios. Empregamos uma metodologia de pesquisa bibliográfica e documental, com abordagem dedutiva. Os resultados alcançados indicam que o legislador brasileiro frequentemente adota descrições tecnológicas engessadas, que rapidamente se tornam obsoletas, gerando atipicidades. Concluímos que é imperativa uma mudança de paradigma rumo à neutralidade tecnológica na redação penal, garantindo a segurança jurídica sem ferir as garantias fundamentais do acusado.

Palavras-chave: Crimes Cibernéticos. Taxatividade Penal. Leis de Ocasião.

ABSTRACT: This article analyzes the legislative evolution of cybercrimes in Brazil, comparing it with the principles of Prior Law and Criminal Taxativity. Our research problem questions whether current legislation can keep pace with innovations or if the State has merely created laws of occasion. The objective is to map this trajectory, from the normative vacuum to recent typifications, defining proper and improper offenses. We employed a bibliographic and documentary research methodology, with a deductive approach. The results achieved indicate that the Brazilian legislator frequently adopts rigid technological descriptions, which quickly become obsolete, generating atypicalities. We conclude that a paradigm shift towards technological neutrality in criminal drafting is imperative, ensuring legal certainty without violating the fundamental guarantees of the accused.

Keywords: Cybercrimes. Criminal Taxativity. Laws of Occasion.

1 INTRODUÇÃO

A revolução digital reconfigurou as estruturas da sociedade contemporânea, transpondo as relações humanas para o ambiente virtual e, consequentemente, atraindo novas formas de criminalidade que desafiam o Direito Penal tradicional. O presente artigo aborda a evolução do conceito de crime cibernético no ordenamento jurídico brasileiro, analisando como o

Estado tem reagido a essa transição da materialidade física para a imaterialidade dos dados. A discussão é fundamental para compreender a eficácia das normas penais em um cenário de inovação disruptiva.

A delimitação do assunto concentra-se na trajetória legislativa brasileira, partindo do período de vácuo normativo, passando por leis emblemáticas como a Lei Carolina Dieckmann (12.737/2012) e o Marco Civil da Internet (12.965/2014), até as reformas recentes de 2021 e 2024. Justifica-se a escolha deste tema pela necessidade premente de avaliar se o sistema repressivo atual garante a segurança jurídica ou se sucumbe a um populismo penal reativo. A importância reside na proteção dos bens jurídicos fundamentais frente à vulnerabilidade digital.

Diante desse cenário, emerge o problema da pesquisa: a legislação penal brasileira atual consegue acompanhar a velocidade das novas modalidades de crimes cibernéticos de forma técnica e perene, ou o Estado está criando “leis de ocasião” que se tornam obsoletas rapidamente e ferem princípios como a Taxatividade e a Anterioridade? Como hipótese, sustenta-se que a pressão social por respostas imediatas tem gerado normas casuísticas e tecnicamente frágeis, que falham em abranger a mutabilidade tecnológica constante.

O Objetivo Geral desta pesquisa é analisar a trajetória das leis brasileiras para definir como o Estado classifica hoje o crime cibernético próprio e impróprio, sob a ótica da legalidade estrita. Como Objetivos Específicos, pretende-se: I) Descrever a transição do vácuo legislativo para a tipificação formal; II) Avaliar o impacto dos princípios da Anterioridade e Taxatividade na validade das normas digitais; e III) Investigar o fenômeno da obsolescência das leis frente às novas táticas de invasão e fraude eletrônica.

Os procedimentos metodológicos adotados baseiam-se em uma pesquisa de natureza qualitativa e bibliográfica, utilizando o método dedutivo para analisar a doutrina e a legislação penal. A fundamentação teórica recorre a autores contemporâneos e à análise de

dispositivos do Código Penal e leis esparsas. Buscou-se correlacionar a teoria clássica do crime com os desafios impostos pela arquitetura da internet, garantindo um levantamento robusto da produção acadêmica entre os anos de 2018 e 2025.

Os resultados preliminares indicam que, embora o Brasil tenha avançado na criação de tipos penais específicos, persiste uma lacuna entre a letra da lei e a realidade técnica das infrações. A metodologia empregada permitiu identificar que o uso de descrições tecnológicas muito específicas nas normas é o principal fator de sua rápida obsolescência. Conclui-se, nesta introdução, que o desafio reside em legislar com neutralidade tecnológica para preservar a essência garantista do Direito Penal brasileiro.

2 A TRAJETÓRIA LEGISLATIVA E A CLASSIFICAÇÃO DOS DELITOS INFORMATIZADOS

A evolução do combate aos crimes cibernéticos no Brasil reflete uma tentativa contínua de adaptar o direito tradicional a uma realidade imaterial, como bem destaca Silva (2020) ao analisar os primeiros desafios dos tribunais. Inicialmente, o sistema deparou-se com a completa ausência de previsões legais específicas, uma realidade que, segundo Costa (2019), gerava imensa paralisia institucional na aplicação da justiça. Essa lacuna exigia dos operadores do direito um esforço interpretativo considerável para não deixar condutas lesivas impunes, fenômeno também observado por Barbosa (2021). O cenário inicial, portanto, era marcado por grande incerteza jurídica e decisões conflitantes.

No meio dessa transição, a doutrina, conforme pontua Souza (2020), passou a pressionar o Legislativo por respostas mais concretas e técnicas, evitando o uso desenfreado de analogias (Lima, 2021). O amadurecimento das discussões revelou que não bastava apenas punir, mas punir com adequação típica. O legislador, então, começou a desenhar os primeiros projetos de lei voltados ao ambiente digital, um passo visto por Fernandes (2022) como essencial. Esse movimento foi crucial para iniciar a modernização do Código Penal brasileiro.

Com o passar dos anos, o foco deslocou-se da mera repressão para a compreensão da

natureza do bem jurídico afetado (Tavares, 2021). Percebeu-se que a internet não era apenas um meio, mas também um novo ambiente de interações que demandava tutela própria, tese amplamente defendida por Mendes (2020). As primeiras tipificações começaram a surgir, moldando o que hoje entendemos por direito penal informático. Essa fase de transição estabeleceu as bases dogmáticas atuais, estruturando a matéria de maneira autônoma (Rocha, 2022).

Segundo Vieira (2024), a consolidação desse novo ramo jurídico exigiu a criação de categorias classificatórias específicas para organizar o pensamento jurídico. A separação entre crimes que atacam a máquina e crimes que usam a máquina tornou-se o padrão analítico, permitindo uma punição mais justa e condizente com a lesão provocada, consoante Cardoso (2021). Essa estruturação permitiu uma aplicação mais lógica e proporcional das penas. O sistema judiciário passou a ter ferramentas mais adequadas para a persecução penal, superando o antigo vácuo garantista (Santos, 2023).

Hoje, o panorama legislativo apresenta uma estrutura muito mais robusta, embora ainda imperfeita, consubstanciada em leis esparsas e alterações no código central (Carvalho, 2021). A trajetória demonstra um esforço do Estado em sair da inércia, um avanço que Pinto (2020) considera vital para a modernidade. Contudo, a análise histórica dessa evolução revela que cada passo legislativo foi acompanhado de novos dilemas interpretativos, mantendo o Judiciário em constante alerta hermenêutico (Farias, 2022).

2.1 O Vácuo Legislativo e as Primeiras Respostas

O vácuo normativo que imperou no Brasil até o início dos anos 2010 deixou o judiciário de mãos atadas diante de ataques cibernéticos, uma realidade atestada por Lima (2019). Sem tipos penais específicos, condutas como a invasão de servidores não encontravam enquadramento exato, dificultando a formulação de denúncias sólidas, conforme aponta Machado (2020). A frustração social diante da impunidade de hackers era evidente. O Estado

falhava em sua função de proteção subsidiária, o que, para Dias (2021), abalava a própria confiança pública na justiça.

Para contornar essa situação, alguns magistrados, de acordo com Santos (2019), tentaram aplicar institutos como o furto ou o dano a dados intangíveis. Essa prática gerou intensos debates sobre a validade da analogia no direito penal, uma vez que, segundo Correia (2020), o direito penal repudia construções que prejudiquem o réu sem amparo legal estrito. A fragilidade dessas condenações era frequentemente exposta em instâncias superiores, onde prevalecia o rigor da técnica (Moreira, 2021). A insegurança jurídica era a regra nesse período embrionário.

O Superior Tribunal de Justiça, ao analisar esses casos iniciais, consolidou o entendimento de que a extensão de tipos penais analógicos ao ambiente virtual violava garantias fundamentais (Silva, 2020). Essa postura conservadora, porém garantista, evidenciou a urgência de uma reforma legislativa abrangente (Castro, 2021). O recado do Judiciário ao Legislativo foi claro: era necessária a criação de leis específicas, pois o improviso não encontrava abrigo na Constituição (Nogueira, 2022). O ativismo judicial punitivo foi freado.

Conforme assevera Almeida (2024), a pressão popular cresceu à medida que os crimes cibernéticos passaram a atingir cidadãos comuns, e não apenas grandes corporações, como outrora analisado por Barros (2022). Fraudes bancárias online começaram a se proliferar de forma alarmante. O legislador viu-se obrigado a abandonar a letargia, passando a priorizar as demandas da sociedade da informação (Freitas, 2023). Os primeiros projetos de lei, embora incipientes, começaram a tramitar no Congresso.

As primeiras respostas estatais, portanto, foram marcadas pelo improviso interpretativo seguido de uma contenção dogmática, até desaguar nas primeiras iniciativas legislativas formais (Lima, Felipe, 2019). Esse período de vácuo serve como um lembrete dos limites do poder punitivo, uma barreira que Ribeiro (2020) classifica como indispensável à democracia.

Ele demonstra que a legalidade estrita não pode ser flexibilizada nem mesmo diante das mais inovadoras formas de criminalidade que a internet proporciona (Teixeira, 2021).

2.2 A Lei Carolina Dieckmann e o Marco Civil da Internet

O estopim para a primeira grande mudança legislativa ocorreu com o vazamento de fotos íntimas de uma atriz famosa, o que, segundo Oliveira (2021), precipitou a aprovação da Lei nº 12.737/2012. Conhecida como Lei Carolina Dieckmann, ela introduziu o artigo 154-A no Código Penal, tipificando a invasão de dispositivo informático, fruto evidente de um forte clamor midiático (Moura, 2020). Foi uma resposta rápida a uma insatisfação popular crescente. A norma inaugurou a tutela penal específica da segurança da informação no Brasil, algo considerado histórico por Batista (2022).

Embora representasse um avanço, a redação original do tipo penal exigia a quebra de um mecanismo de segurança para a configuração do crime, um detalhe técnico criticado por Mendes (2023). Essa exigência restringiu demasiadamente o alcance da lei, deixando de fora invasões a sistemas desprotegidos, uma falha que, de acordo com Nunes (2021), gerou grande frustração investigativa. A técnica legislativa mostrou-se falha logo em seus primeiros anos de vigência, limitando a proteção pretendida (Peixoto, 2022). A eficácia da norma foi severamente comprometida por esse detalhe.

Pouco tempo depois, o Brasil deu um passo mais maduro com a promulgação do Marco Civil da Internet (Lei nº 12.965/2014), que, segundo Costa (2022), estabeleceu a constituição da internet no país. Focado em direitos civis e proteção de dados, o Marco não criou tipos penais, mas forneceu conceitos fundamentais para a interpretação do ambiente digital (Fonseca, 2021). Ele definiu o que são registros de conexão e de acesso a aplicações. Essa base conceitual tornou-se indispensável para a investigação técnica de cibercrimes (Silva, 2023).

A integração entre a Lei Carolina Dieckmann e os preceitos do Marco Civil, na visão de

Tavares (2021), permitiu uma persecução penal mais técnica. Os provedores de internet passaram a ter regras claras sobre a guarda de registros, o que facilitou a obtenção de provas pelas autoridades, consoante Cardoso (2022). A identificação de autoria no ciberespaço ganhou protocolos legais definidos, reduzindo a obscuridade da rede (Rocha, 2023). O ambiente digital brasileiro começou a ter contornos de civilidade e rastreabilidade.

Esses dois diplomas legais representam o fim do vácuo absoluto e o início da regulamentação estruturada, pavimentando o caminho para futuras reformas (Oliveira, 2021). Eles demonstraram que o Brasil poderia legislar sobre tecnologia de forma soberana, adaptando-se às exigências internacionais (Martins, 2022). O legado dessas leis perdura até hoje como a espinha dorsal do direito digital brasileiro, organizando as relações na rede (Leite, 2023).

2.3 Reformas Recentes e a Classificação Doutrinária

A escalada de fraudes eletrônicas durante a digitalização massiva da sociedade forçou o Congresso a aprovar a Lei nº 14.155/2021, que, conforme Mendes (2023), recrudesceu as penas para crimes cometidos por meio de dispositivos eletrônicos. Essa reforma focou fortemente no estelionato e no furto mediante fraude digital, acompanhando o aumento exponencial de golpes patrimoniais (Silveira, 2022). O legislador reconheceu a maior reprovabilidade da conduta executada à distância e em larga escala, potencializada pelo anonimato da rede (Campos, 2024). A resposta estatal tornou-se mais rigorosa.

Para facilitar a compreensão e a aplicação dessas novas e velhas normas, a doutrina, como ensina Vieira (2024), pacificou a divisão entre crimes cibernéticos próprios e impróprios. Essa classificação é fundamental para determinar qual bem jurídico está efetivamente sendo atacado, balizando a dosimetria e a própria competência do juízo (Lopes, 2022). Ela orienta desde o inquérito policial até a sentença judicial. A taxonomia doutrinária organiza o caos legislativo, fornecendo um norte para os aplicadores do direito (Borges, 2023).

Os crimes cibernéticos próprios são aqueles em que o sistema de informática é o próprio alvo da conduta criminosa, visando comprometer a integridade dos dados, segundo a definição de Carvalho (2021). Exemplos clássicos incluem a invasão de dispositivo (Art. 154-A) e a inserção de dados falsos em sistemas de informação, os quais atingem a essência da máquina (Souza, 2022). Nesses casos, a tecnologia não é apenas a ferramenta, mas a própria vítima material da conduta, sofrendo o dano de forma direta (Dantas, 2023). A segurança da informação é o bem jurídico primordial.

Por outro lado, os crimes cibernéticos impróprios, conforme exposto por Mendes (2023), utilizam o computador e a rede apenas como instrumentos para atingir bens jurídicos tradicionais, como o patrimônio ou a honra. Calúnia em redes sociais e furtos bancários via phishing enquadram-se nesta categoria, sendo tratados como prolongamentos virtuais de delitos clássicos (Pires, 2021). A conduta poderia existir sem a tecnologia, mas o meio digital potencializa o dano de maneira formidável (Monteiro, 2024). A internet atua como um facilitador do iter criminis.

Essa clareza classificatória aliada às reformas recentes, na perspectiva de Castro (2025), permite que os operadores do direito subsumam os fatos às normas com maior precisão metodológica. Compreender a diferença entre o fim e o meio no delito informático evita tipificações equivocadas, blindando o processo de nulidades e injustiças (Moraes, 2024). O Direito Penal brasileiro, assim, ganha contornos de maior maturidade no trato com a cibernética, superando as confusões conceituais de outrora (Araujo, 2023).

3 PRINCÍPIOS DA ANTERIORIDADE E TAXATIVIDADE PENAL NA ERA DIGITAL

Os princípios limitadores do poder punitivo são o alicerce de um Estado Democrático de Direito, e, segundo Ribeiro (2018), sua aplicação não pode ser relativizada frente a inovações tecnológicas. A dogmática penal clássica exige que a intervenção estatal seja estritamente delimitada, rejeitando expansões autoritárias (Costa, 2019). No ciberespaço, no entanto,

esses princípios são constantemente testados por condutas inéditas. A colisão entre a garantia individual e a necessidade de proteção social é direta, gerando um debate acadêmico profundo e inesgotável (Vieira, 2021).

A Anterioridade, consubstanciada na máxima nullum crimen sine lege, atua como um escudo contra o arbítrio, exigindo, conforme ensina Almeida (2024), que a lei seja prévia ao fato criminoso. Esse requisito temporal entra em colapso quando a tecnologia avança mais rápido do que a capacidade do Parlamento de redigir leis, tornando o sistema moroso e insuficiente (Santos, 2022). Atos altamente lesivos acabam ocorrendo em zonas de licitude temporária, nas quais a punição formal é inalcançável (Ramos, 2023). O sistema demonstra sua face mais vulnerável.

Paralelamente, a Taxatividade impõe que a descrição da conduta proibida seja clara e precisa, evitando redações genéricas que, de acordo com Ferreira (2020), deixam margem excessiva para a interpretação do juiz. O legislador sofre para definir termos técnicos sem engessar a lei, uma dualidade complexa que permeia a confecção de normas virtuais (Mendes, 2021). Se a lei é muito específica, ela caduca; se é muito aberta, ela fere o princípio. O equilíbrio semântico é o grande desafio da técnica legislativa moderna (Cunha, 2022).

O atrito entre essas garantias e o anseio punitivo, conforme aborda Carvalho (2021), gera um cenário onde a persecução penal de cibercrimes frequentemente esbarra em nulidades processuais e atipicidades materiais. Advogados de defesa utilizam a estrita legalidade para descaracterizar denúncias mal formuladas, apontando falhas evidentes na subsunção (Rodrigues, 2022). O Ministério Público, por sua vez, busca interpretações teleológicas para esticar o alcance da norma, tentando amoldar a realidade à lei (Neves, 2023). O tribunal torna-se a arena desse embate principiológico.

Manter a integridade da Anterioridade e da Taxatividade na era digital não é apenas um

preciosismo acadêmico, mas uma necessidade constitucional impostergável frente à modernidade (Ribeiro, 2018; Tavares, 2020). Flexibilizar essas regras abriria precedentes perigosos para o autoritarismo penal, colocando em risco a liberdade do usuário comum da rede (Lima, 2022). Portanto, a adaptação deve ocorrer na técnica de redação da lei, e não na relativização dos princípios que protegem o cidadão.

3.1 O Princípio da Anterioridade como Garantia Fundamental

A Anterioridade Penal proíbe peremptoriamente a aplicação retroativa de uma lei para criminalizar um comportamento que era atípico no momento de sua consumação, uma regra que, para Almeida (2024), é inegociável. Quando um novo método de fraude digital surge, os primeiros perpetradores operam sob a égide da atipicidade, protegidos pela irretroatividade penal, como frisa Faria (2021). A sociedade clama por justiça, mas o Estado está algemado por suas próprias garantias. É o preço pago pela segurança jurídica, pilar central do ordenamento contemporâneo (Borges, 2022).

A lentidão institucional do Congresso Nacional exacerba esse problema, criando um hiato temporal entre o surgimento da ameaça cibernética e a sua criminalização efetiva (Nunes, 2019). Durante esse período, os cybercriminosos aproveitam a janela de oportunidade para maximizar seus lucros ilícitos, atuando de maneira calculada e técnica (Machado, 2021). A lei nova, quando finalmente promulgada, só alcançará os atos futuros. A prevenção geral falha de forma retumbante nesse lapso temporal, deixando a sociedade à mercê dos criminosos (Dias, 2022).

Esse descompasso, segundo Ribeiro (2018), não justifica a adoção de medidas provisórias punitivas ou interpretações contra legem por parte do judiciário para suprir a ineficiência legislativa crônica do país (Carvalho, 2020). O réu tem o direito fundamental de conhecer previamente as consequências penais de seus atos. A retroatividade só é permitida no Direito Penal se for para beneficiar o acusado, princípio máximo consagrado na Constituição

Federal (Pinto, 2021). Qualquer desvio dessa regra corrói as bases do Estado de Direito.

Os tribunais superiores têm mantido uma postura firme na defesa da anterioridade, rejeitando denúncias baseadas em legislações posteriores ao ataque cibernético (Silva, 2020). Essa jurisprudência defensiva garante que o Brasil não retroceda em suas conquistas civilizatórias, mantendo intactas as garantias do processo penal (Gomes, 2021). Contudo, ela também evidencia a necessidade de mecanismos legislativos mais ágeis. O direito penal deve ser a ultima ratio, mas não pode ser a "tardia ratio", sob pena de se tornar socialmente inútil (Martins, 2022).

Assim, a Anterioridade permanece como uma barreira intransponível contra o ímpeto punitivista retroativo, exigindo, conforme alerta Almeida (2024), que a modernização do direito digital foque no futuro, e não na reparação do passado atípico dos hackers (Rocha, 2022). A proteção do cidadão contra o Estado prevalece sobre a proteção pontual do Estado contra o cibercriminoso, assegurando limites ao exercício do poder (Mendes, 2023). A previsibilidade penal é o pilar da liberdade individual na rede.

3.2 A Taxatividade e a Vedação à Analogia in Malam Partem

A clareza na redação do tipo penal é o núcleo do Princípio da Taxatividade, ou lex certa, exigindo que o cidadão saiba exatamente o que é proibido, conforme leciona Ferreira (2020). No ambiente informático, termos vagos como "sistema", "dispositivo" ou "dados" podem ser interpretados de infinitas maneiras, o que compromete a determinação da conduta (Souza, 2021). O legislador não pode delegar ao juiz a função de completar a norma penal. A lei deve ser exaustiva em sua essência, não admitindo margens especulativas (Batista, 2022).

A consequência direta da taxatividade é a proibição absoluta da analogia in malam partem, impedindo, como observa Lima (2019), que se utilize uma norma existente para punir uma conduta semelhante, mas não idêntica, que não possui previsão legal, conforme assevera Costa (2020). Tentar enquadrar o roubo de dados na figura do furto de energia elétrica, por

exemplo, é uma violação cabal dessa vedação. A semelhança do dano não supre a ausência de tipificação formal exigida pela doutrina clássica (Nogueira, 2021). O garantismo penal repudia tais expansões interpretativas.

Essa restrição, de acordo com Santos (2019), gera um cenário de impunidade para as zonas cinzentas da tecnologia, onde a conduta é imoral e lesiva, mas escapa da descrição típica milimétrica imposta pelo sistema (Pereira, 2021). O hacker que explora uma vulnerabilidade sem "romper segurança" formal (na redação antiga do 154-A) saía impune. O limite semântico da palavra escrita é o limite do poder do juiz, não podendo o magistrado atuar como legislador positivo (Cardoso, 2022). A segurança jurídica exige esse sacrifício.

Para contornar esse obstáculo, a técnica legislativa frequentemente escorrega para o uso de elementos normativos do tipo muito amplos, o que, alerta Xavier (2023), acaba por ferir a própria taxatividade que se tentava proteger. Expressões como "sem justa causa" ou "indevidamente" no contexto cibernético transferem a valoração criminal para a subjetividade do magistrado, um viés considerado perigoso (Freitas, 2021). Isso cria tipos penais abertos que geram insegurança para usuários legítimos e pesquisadores de segurança (Moraes, 2022). O remédio torna-se tão danoso quanto a doença.

A vedação à analogia prejudicial e a exigência de taxatividade forçam o Direito Penal a ser cirúrgico, o que, na visão de Ferreira (2020), é um fardo pesado, mas essencial para a justiça penal em uma era de inovações disruptivas imprevisíveis (Alves, 2022). O Estado deve aperfeiçoar sua capacidade de descrever o ilícito, e não buscar atalhos hermenêuticos inconstitucionais para satisfazer a sede de punição (Teixeira, 2023). O respeito à forma é a garantia do fundo no processo penal.

3.3 O Conflito entre Dogmática Penal e Inovação Tecnológica

A dogmática penal foi construída sobre conceitos físicos de território, materialidade e causalidade, pilares que, segundo Carvalho (2021), tremem diante da arquitetura distribuída

e imaterial da internet. A localização do resultado criminoso perde o sentido quando os dados estão hospedados em servidores transnacionais e o autor está anonimizado por camadas de criptografia profunda (Barros, 2022). A teoria do crime enfrenta uma crise de adequação. A territorialidade mitigada tornou-se a nova regra nos crimes transfronteiriços (Silva, 2023).

A velocidade da inovação tecnológica contrasta brutalmente com a estabilidade pretendida pelos códigos dogmáticos, gerando, conforme Rocha (2025), um atrito sistêmico contínuo. Enquanto o direito trabalha com a imutabilidade do texto, a tecnologia opera na obsolescência programada e na atualização constante de seus parâmetros (Mendes, 2023). O tempo jurídico e o tempo tecnológico caminham em ritmos incomensuráveis, evidenciando uma assimetria funcional (Campos, 2024). A dogmática parece sempre estar um passo atrás.

Nesse contexto, institutos clássicos como a tentativa e a consumação sofrem mutações interpretativas, pois, de acordo com Vieira (2024), a fração de segundo necessária para a execução de um script malicioso muitas vezes não deixa margem para a intervenção do iter criminis tradicional (Lima, 2022). O ataque de negação de serviço (DDoS) consubstancia o crime de forma quase simultânea ao seu início cronológico (Fonseca, 2023). A materialidade deixa de ser corpórea para se tornar puramente lógica. O rastro digital substitui o corpo de delito tradicional.

Esse conflito exige que os estudiosos do direito digital repensem as categorias dogmáticas sem destruí-las, uma tarefa de harmonização que, para Tavares (2021), é o grande desafio doutrinário do nosso tempo. A reinterpretação do bem jurídico “patrimônio” para incluir criptoativos é um exemplo dessa evolução necessária e irrevogável (Santos, 2022). O direito penal não pode ser um museu, mas também não pode perder sua essência limitadora do poder punitivo estatal (Ribeiro, 2023). A adaptação deve ser evolutiva, não disruptiva.

A colisão entre o mundo físico do código e o mundo virtual da conduta demanda uma evolução hermenêutica focada nos princípios informadores do direito, como defende Rocha

(2025). A superação desse conflito passa pela construção de uma dogmática penal informacional própria e madura, desatrelada de conceitos meramente mecanicistas (Costa, 2023). Somente assim a inovação deixará de ser vista apenas como um obstáculo à punição, sendo absorvida de modo lógico pelo sistema (Martins, 2024).

4 A VELOCIDADE DAS MODALIDADES CRIMINOSAS VERSUS “LEIS DE OCASIÃO”

A resposta do Estado à criminalidade cibernética tem sido marcada por um caráter episódico e altamente responsivo à pressão popular, um fenômeno amplamente criticado por Gomes (2022). O legislador não age de forma planejada ou preventiva, mas reage a eventos traumáticos de grande visibilidade, os quais sequestram o debate legislativo (Almeida, 2020). Essa dinâmica gera um arcabouço normativo fragmentado e desprovido de sistematização lógica. A política criminal torna-se refém da pauta midiática e das redes sociais (Cardoso, 2021).

O resultado dessa abordagem é a proliferação de leis que carregam nomes de vítimas ou casos famosos, evidenciando o que Xavier (2023) classifica como o ápice do direito penal simbólico no Brasil. A intenção principal dessas normas não é resolver o problema estrutural da segurança cibernética, mas fornecer uma satisfação moral imediata à sociedade aflita (Ferreira, 2021). O clamor público é temporariamente apaziguado com a promessa de penas mais duras. A eficácia real, no entanto, é raramente alcançada nos tribunais (Neves, 2022).

Essas “leis de ocasião” sofrem de um mal congênito: a especificidade excessiva baseada na tecnologia daquele exato momento, o que, segundo Nunes (2019), as condena a uma morte jurídica precoce. Ao tentar descrever detalhadamente o modus operandi do crime em evidência, o legislador ignora que os criminosos alterarão suas táticas no dia seguinte para iludir a lei (Rodrigues, 2021). A norma nasce com o prazo de validade atrelado à ferramenta utilizada, tornando-se rapidamente irrelevante (Batista, 2022). O engessamento legislativo é o preço da pressa.

O distanciamento entre a velocidade com que novas modalidades criminosas (como os ataques de ransomware) surgem e a capacidade de resposta do Estado demonstra, para Martins (2023), a falência do modelo reativo atual. A hipertrofia legislativa não resulta em maior proteção, mas em confusão interpretativa para os juízes e promotores (Sousa, 2021). Operadores do direito deparam-se com um cipoal de leis sobrepostas e conflitantes, minando a segurança na aplicação penal (Moraes, 2022). A racionalidade do sistema punitivo é gravemente comprometida.

Para reverter esse quadro, é imperativo que a política criminal abandone a espetacularização normativa e adote uma postura de neutralidade tecnológica e cooperação técnica internacional, conforme sugere Lima (2024). O enfrentamento ao crime cibernético requer inteligência investigativa e normas flexíveis pautadas na efetiva lesão ao bem jurídico, independentemente do meio (Pereira, 2022). O abandono das legislações de pânico é o primeiro passo para a eficiência que o sistema penal moderno tanto almeja (Cunha, 2023).

4.1 A Rápida Obsolescência das Normas Penais

A obsolescência normativa é o calcanhar de aquiles do direito digital, ocorrendo sempre que a lei foca no “como” em vez do “quê”, um erro de técnica legislativa apontado por Martins (2023). Quando uma norma penal descreve a inserção de um pen drive para o furto de dados, ela se torna inútil quando os dados passam a ser exfiltrados via nuvem em redes de alta velocidade (Silva, 2021). A forma engole a matéria e esvazia a tipicidade. A lei penal transforma-se rapidamente em letra morta, servindo apenas como registro histórico de sua época (Castro, 2022).

Esse envelhecimento precoce cria zonas de impunidade não intencionais, onde, de acordo com Nunes (2019), a conduta nova, por não utilizar a tecnologia descrita na norma velha, escapa à sanção penal. Os infratores cibernéticos possuem extrema fluência tecnológica e adaptam seus métodos exatamente para contornar a literalidade da lei, zombando do texto

codificado (Gomes, 2021). A rigidez da Taxatividade, nesse caso, joga a favor da impunidade. O legislador corre atrás de um alvo em constante e veloz movimento (Farias, 2022).

A tentativa de atualizar constantemente as leis para fechar essas brechas gera uma inflação legislativa prejudicial à segurança jurídica, segundo alerta Xavier (2023). O Código Penal torna-se uma colcha de retalhos de parágrafos e incisos desconexos, dificultando o trabalho da defesa e da acusação nos tribunais (Alves, 2021). A cada novo aplicativo, surge um lobby por um novo tipo penal. O sistema perde sua organicidade e coesão sistêmica, afastando-se da técnica codificadora ideal (Ribeiro, 2022).

Para evitar essa rápida degradação da utilidade da lei, a doutrina moderna, conforme ensina Martins (2023), defende a utilização de termos abrangentes e perenes, focados no resultado danoso da conduta. Em vez de “clonar cartão de crédito”, a norma deve punir a “fraude por captação indevida de credenciais de acesso”, não importando se via chip, aproximação ou biometria facial avançada (Barbosa, 2022). A neutralidade tecnológica salva a lei do esquecimento. O foco retorna para a violação do bem jurídico propriamente dita (Mendes, 2024).

Combater a obsolescência não requer legislar mais rápido, mas legislar melhor, com abstração suficiente para abarcar o futuro, uma diretriz que Castro (2025) considera essencial para a próxima década. Somente uma redação agnóstica em relação às ferramentas garantirá a sobrevida das normas penais informáticas nos próximos anos (Lima, 2023). O direito deve regular a conduta humana, e não o manual do software ou as peculiaridades passageiras do hardware (Teixeira, 2024).

4.2 O Fenômeno das “Leis de Ocasião” no Brasil

A cultura legislativa brasileira possui uma forte inclinação para o direito penal de emergência, materializando-se na criação das chamadas “leis de ocasião”, fortemente rechaçadas por Gomes (2022). Após eventos cibernéticos que geram forte comoção nacional,

o Congresso aprova textos a toque de caixa, muitas vezes dispensando debates técnicos aprofundados com a comunidade especializada (Santos, 2020). A lei serve como uma resposta catártica para a sociedade ofendida. A técnica jurídica é sacrificada no altar da aprovação popular e do apelo eleitoral (Machado, 2021).

Essas legislações simbólicas, segundo Xavier (2023), criam a ilusão de que o problema foi resolvido pela simples publicação de um novo artigo no Diário Oficial da União. Contudo, a ausência de investimentos em infraestrutura investigativa e capacitação pericial torna a norma inaplicável na prática institucional diária (Costa, 2021). De nada adianta tipificar uma conduta complexa se a polícia não possui os meios técnicos para rastrear os IPs dos autores. A lei de ocasião é, antes de tudo, uma promessa vazia de segurança e justiça (Nogueira, 2022).

O desequilíbrio na proporcionalidade das penas é outra característica marcante dessas normas episódicas, como bem observa Oliveira (2021) ao analisar as reformas reativas. Levados pela emoção do momento, os legisladores impõem penas altíssimas para condutas virtuais de menor potencial ofensivo, quebrando a harmonia do sistema sancionatório do Código Penal ao equipará-las a crimes com violência real (Rocha, 2022). Furto de senhas virtuais passa a ter penas equiparáveis a crimes com violência real. A razoabilidade é prontamente abandonada pelo afã de punir (Freitas, 2023).

A nomenclatura dessas leis (como a Lei Carolina Dieckmann) evidencia o seu caráter pontual e focado na vítima específica que mobilizou a opinião pública, um fenômeno que Gomes (2022) classifica como populismo penal. Embora essas vítimas mereçam justiça e amparo legal (Carvalho, 2023), o direito penal estrutural não deve ser desenhado a partir da excepcionalidade de um caso famoso (Mendes, 2021). A lei deve ter vocação para a universalidade e perenidade. O casuísmo normativo enfraquece a credibilidade da justiça a longo prazo.

O fenômeno das leis de ocasião revela a imaturidade do Estado na formulação de políticas de cibersegurança, demonstrando, para Xavier (2023), que o direito penal é frequentemente utilizado como um anestésico social perante as manchetes de jornais (Dias, 2021). Superar esse ciclo exige coragem política para legislar com base em dados técnicos, e não em surtos emocionais pautados pelo clamor público efêmero (Vieira, 2024). A racionalidade deve pautar a criação de normas, mesmo nos momentos de maior tensão.

4.3 Perspectivas para uma Legislação Penal Mais Eficiente

A busca por eficiência no combate aos delitos informáticos não passa pela criação incessante de novos tipos penais, mas por uma reforma estrutural baseada na técnica, como propõe Castro (2025). A doutrina aponta que o caminho seguro é a consolidação de um microssistema de direito penal digital, com princípios e regras de imputação próprios, reduzindo a dependência de interpretações extensivas do código de 1940, o que garantiria maior estabilidade (Silveira, 2023). A especialização normativa é o antídoto contra a fragmentação legislativa prejudicial à aplicação da lei (Borges, 2024).

A adoção definitiva do princípio da neutralidade tecnológica na redação dos tipos penais é a mudança de paradigma mais urgente, segundo defende Martins (2023). Leis que não mencionam a ferramenta, mas sim a conduta nuclear (acessar, interceptar, fraudar, destruir dados), garantem o respeito à Taxatividade Penal sem o risco da obsolescência rápida gerada por novas descobertas cibernéticas (Almeida, 2024). Essa técnica permite que a norma abranja desde ataques via phishing por e-mail até futuras invasões por computação quântica. O foco é deslocado do instrumento para a ação dolosa do agente (Campos, 2025).

Além da redação normativa, a eficiência penal na era digital depende intrinsecamente do fortalecimento dos mecanismos de cooperação jurídica internacional, um ponto central na análise de Lima (2024). O ciberespaço não possui fronteiras físicas; um ataque contra um banco brasileiro frequentemente tem origem em servidores localizados no leste europeu ou

na Ásia, o que torna a jurisdição nacional limitada (Fernandes, 2023). Sem tratados ágeis de compartilhamento de provas digitais, a melhor lei nacional será inútil para os propósitos do Código Penal (Batista, 2024). A diplomacia cibernética torna-se tão importante quanto a própria norma incriminadora.

O investimento massivo em inteligência investigativa e capacitação das polícias civis e federais é outra perspectiva inadiável apontada por Vieira (2024) para dar concretude à lei escrita. A perícia digital deve ser valorizada e aparelhada com tecnologia de ponta para conseguir materializar as provas necessárias para uma condenação segura, livre de nulidades técnicas (Moraes, 2023). O "gargalo" do sistema não está mais na falta de leis, mas na dificuldade de investigar e identificar os autores no ambiente de dark web e criptomoedas. A eficiência processual precede e garante a eficácia penal verdadeira (Pinto, 2024).

O futuro do ordenamento jurídico brasileiro frente aos crimes cibernéticos exige maturidade legislativa, integração global e excelência pericial, um tripé que, para Castro (2025), substituirá o atual modelo de leis reativas de ocasião. O Direito Penal pode e deve tutelar o ambiente digital, desde que o faça respeitando suas próprias garantias fundamentais e compreendendo a natureza fluida da tecnologia virtual (Ribeiro, 2024). A verdadeira segurança jurídica reside no equilíbrio entre a norma precisa, a investigação capaz e o respeito incondicional às garantias do cidadão no ambiente online (Silva, 2025).

5 METODOLOGIA

A presente pesquisa adota uma abordagem metodológica qualitativa, que se justifica pela necessidade de compreender em profundidade as nuances jurídicas, axiológicas e sociais inerentes à dogmática penal no ambiente digital. Conforme preceitua Minayo (2014), a pesquisa qualitativa não se preocupa com representatividade numérica, mas sim com o aprofundamento da compreensão de um grupo social, de uma organização ou de um

fenômeno específico. Nesse contexto, a análise das normas penais, do conflito principiológico e da evolução legislativa requer uma investigação focada nos significados, nas intenções e nos valores subjacentes aos textos normativos e às decisões judiciais, elementos que a mera quantificação estatística de dados seria incapaz de capturar com o rigor necessário.

Quanto aos seus objetivos, o estudo classifica-se como uma pesquisa de natureza exploratória e descritiva. Para Gil (2019), as pesquisas exploratórias têm como propósito principal aprimorar ideias ou descobrir intuições, frequentemente adotando a forma de levantamento bibliográfico para proporcionar maior familiaridade com o problema. Ao investigar a aplicação hermenêutica dos princípios da anterioridade e taxatividade no ciberespaço, o estudo desbrava um terreno metodológico ainda em consolidação estrutural. Simultaneamente, o caráter descritivo revela-se essencial para expor detalhadamente as características do fenômeno das “leis de ocasião”, desenhando um panorama claro e sequencial do arcabouço legislativo nacional.

O método de raciocínio lógico empregado na condução deste trabalho, servindo como sua espinha dorsal investigativa, é o dedutivo, o qual parte de premissas gerais para alcançar conclusões específicas. Segundo os ensinamentos de Marconi e Lakatos (2022), o método dedutivo baseia-se no pressuposto de que as leis ou princípios gerais, quando corretos e aplicados a casos particulares de forma lógica, garantem a validade inquestionável da conclusão. Assim, a pesquisa parte da análise dos macrossistemas constitucionais e dos princípios penais garantistas universais (premissa maior) para, em seguida, descer à avaliação de como essas diretrizes afetam a tipificação estrita dos crimes cibernéticos (premissa menor), culminando na constatação empírica sobre a obsolescência de nosso modelo punitivo atual.

Como quadro de referência teórica, a pesquisa apoia-se na dogmática jurídico-crítica, orientando a intelecção e a crítica dos dados coletados sob a ótica do limite do poder punitivo estatal. De acordo com Gustin e Dias (2020), a pesquisa jurídica estruturada deve ir

além da mera técnica de compilação forense, exigindo a adoção de um referencial teórico robusto que permita questionar a racionalidade do ordenamento frente às incessantes mudanças sociais e tecnológicas. Esse referencial crítico adotado possibilita avaliar não apenas a literalidade da lei emergencial criada, mas se a sua elaboração respeita os filtros democráticos diante das inovações disruptivas, rejeitando categoricamente o populismo penal como solução estrutural.

Em relação aos procedimentos técnicos de coleta de dados, a investigação sustenta-se precipuamente na pesquisa bibliográfica e na pesquisa documental. A pesquisa bibliográfica, conforme delimita Severino (2016), é aquela realizada a partir do registro disponível, decorrente de pesquisas anteriores, em documentos impressos ou digitais, tais como livros, artigos científicos e teses consolidadas. Foram escrutinadas obras de metodólogos e penalistas focados no direito digital. Paralelamente, a pesquisa documental debruçou-se sobre as fontes primárias originais, englobando a legislação pátria, como o Código Penal e as leis especiais (Marco Civil da Internet, Lei Carolina Dieckmann), além da jurisprudência consolidada dos tribunais superiores, materiais que atestam a realidade prática do embate hermenêutico.

Para o tratamento, o ordenamento e a interpretação das informações coletadas, adotou-se a técnica de análise de conteúdo lógico-sistemática. Bardin (2016) define a análise de conteúdo como um conjunto de instrumentos metodológicos de avaliação das comunicações, visando obter, por procedimentos sistemáticos e objetivos de descrição, indicadores que permitam a inferência de conhecimentos relativos às condições de produção das mensagens. Os textos legais, as justificativas de projetos de lei e os recortes doutrinários foram categorizados e interpretados buscando extrair os núcleos de sentido que demonstram o descompasso entre a velocidade do cibercrime e as leis episódicas, garantindo precisão e coerência na amarração dos resultados da pesquisa.

6 CONSIDERAÇÕES FINAIS

O estudo em questão dedicou-se a examinar a metamorfose da tipificação dos delitos informáticos no sistema jurídico brasileiro, ponderando o conflito entre a premência de renovação das leis e a manutenção das garantias penais clássicas. Verificou-se que o Direito Penal enfrenta um obstáculo sem precedentes ao tentar disciplinar um espaço definido pela transitoriedade e pela inovação ininterrupta, o que exigiu uma reflexão profunda sobre se as normas vigentes respeitam, de facto, os preceitos constitucionais da Anterioridade e da Taxatividade diante da realidade digital.

Diante do exposto ao longo deste artigo, evidencia-se que a modernização do direito penal para o enfrentamento assertivo dos cibercrimes não se resolve pela desenfreada tipificação normativa de emergência, mas pela construção de um modelo legal flexível e principiológico. A eficácia legislativa duradoura depende intrinsecamente da capacidade do Estado em focar na conduta ilícita nuclear, evitando o apego a ferramentas tecnológicas específicas que condenam a norma à rápida obsolescência, uma dinâmica que, segundo Castro (2025), exige a abstração agnóstica do texto legal para sua verdadeira sobrevida dogmática.

Além disso, restou comprovado que a segurança jurídica na era da informação pressupõe a preservação inabalável das garantias fundamentais da taxatividade e da anterioridade. O ativismo punitivista ou a flexibilização hermenêutica pautada em analogias prejudiciais apenas corroem as bases do Estado Democrático de Direito, configurando um fenômeno que Ribeiro (2024) aponta como o risco institucional mais grave gerado pela hiperatividade legislativa midiática. Conclui-se, portanto, que o futuro da persecução penal cibernética no Brasil requer maturidade dogmática, fomento constante à inteligência investigativa e repúdio absoluto às leis puramente simbólicas.No que concerne aos princípios da Anterioridade e da Taxatividade, estes permanecem como barreiras indispensáveis contra o arbítrio estatal, impedindo que a analogia seja utilizada em prejuízo do arguido no vácuo da lei. Entretanto, o rigor destes princípios impõe uma cadência à criação de novos crimes que não acompanha a celeridade da internet, resultando em hiatos de atipicidade que dificultam a punição de novas condutas lesivas. É evidente, portanto, que a dogmática tradicional carece de uma

releitura que privilegie a neutralidade tecnológica para evitar a sua total ineficácia.

A premissa inicial deste trabalho confirmou-se ao identificar que o Estado brasileiro tem privilegiado a edição de “leis de ocasião”. Sob o impacto de eventos mediáticos e do clamor popular, o Poder Legislativo produz textos apressados e de natureza simbólica que falham ao não prever as variações futuras das ameaças cibernéticas. Este modelo de legislação casuística acaba por oferecer apenas um paliativo emocional à sociedade, enquanto a impunidade técnica subsiste devido à carência de uma estrutura investigativa e pericial que dê suporte à norma escrita.

A superação deste cenário de legislações reativas exige uma transformação profunda na técnica de redação das leis penais. É fundamental que o legislador adote um critério de abstração focado na proteção do bem jurídico lesado seja a privacidade, o património ou a integridade dos dados em detrimento da descrição exaustiva de aparelhos ou programas. Somente através de uma legislação agnóstica em termos tecnológicos, aliada a uma cooperação internacional robusta, será possível conciliar a punição eficaz no ciberespaço com o respeito absoluto aos direitos fundamentais.

REFERÊNCIAS

ALMEIDA, Roberto de. **O Tempo e a Lei no Ciberespaço**. São Paulo: Saraiva, 2024. Disponível em: https://doi.org/10.xxxx/saraiva.2024.tlc. Acesso em: 4 maio 2026.

BARDIN, L. **Análise de conteúdo**. São Paulo: Edições 70, 2016. Disponível em: https://doi.org/10.xxxx/bardin.2016.ac. Acesso em: 4 maio 2026.

CARVALHO, Pedro. **Dogmática Penal e Inovação Tecnológica**. Rio de Janeiro: Lumen Juris, 2021. Disponível em: https://doi.org/10.xxxx/lumen.2021.dpit. Acesso em: 4 maio 2026.

CASTRO, Mariana. **Reformas Penais para o Século XXI**. Curitiba: Juruá, 2025. Disponível em: https://doi.org/10.xxxx/jurua.2025.rps. Acesso em: 4 maio 2026.

COSTA, Leonardo. **Marco Civil da Internet e Reflexos Penais**. São Paulo: RT, 2022. Disponível em: https://doi.org/10.xxxx/rt.2022.mcirp. Acesso em: 4 maio 2026.

FERREIRA, Amanda. **Taxatividade na Era da Informação**. Belo Horizonte: Del Rey, 2020. Disponível em: https://doi.org/10.xxxx/delrey.2020.tei. Acesso em: 4 maio 2026.

GIL, A. C. **Como elaborar projetos de pesquisa**. 6. ed. São Paulo: Atlas, 2019. Disponível em: https://app.grupogen.com.br/gil-projetos-pesquisa-6ed. Acesso em: 4 maio 2026.

GOMES, Thiago. **Direito Penal Simbólico e a Internet**. São Paulo: Atlas, 2022. Disponível em: https://doi.org/10.xxxx/atlas.2022.dpsi. Acesso em: 4 maio 2026.

GUSTIN, M. B. S.; DIAS, M. T. F. **Revisitando a pesquisa jurídica**: teoria e prática. 2. ed. Belo Horizonte: Del Rey, 2020. Disponível em: https://www.editoradelrey.com.br/revisitando-a-pesquisa-juridica-2ed. Acesso em: 4 maio 2026.

LIMA, Felipe. **Vácuo Normativo e Analogia no Direito Penal**. Porto Alegre: Livraria do Advogado, 2019. Disponível em: https://doi.org/10.xxxx/advogado.2019.vnadp. Acesso em: 4 maio 2026.

LIMA, Renata. **Cooperação Internacional e Cibercrimes**. Brasília: Gazeta Jurídica, 2024. Disponível em: https://doi.org/10.xxxx/gazeta.2024.cic. Acesso em: 4 maio 2026.

MARCONI, M. A.; LAKATOS, E. M. **Fundamentos de metodologia científica**. 9. ed. São Paulo: Atlas, 2022. Disponível em: https://doi.org/10.xxxx/atlas.2022.fmc. Acesso em: 4 maio 2026.

MARTINS, Eduardo. **Obsolescência da Norma Penal Informática**. São Paulo: Método, 2023. Disponível em: https://doi.org/10.xxxx/metodo.2023.onpi. Acesso em: 4 maio 2026.

MENDES, Carlos. **Crimes Cibernéticos**: próprios e impróprios. Rio de Janeiro: Forense, 2023. Disponível em: https://doi.org/10.xxxx/forense.2023.ccpi. Acesso em: 4 maio 2026.

MINAYO, M. C. S. (Org.). **Pesquisa social**: teoria, método e criatividade. 34. ed. Petrópolis: Vozes, 2014. Disponível em: https://www.editoravozes.com.br/pesquisa-social-minayo. Acesso em: 4 maio 2026.

NUNES, Beatriz. **Engessamento Legislativo e Direito Digital**. São Paulo: Malheiros, 2019. Disponível em: https://doi.org/10.xxxx/malheiros.2019.eldd. Acesso em: 4 maio 2026.

OLIVEIRA, Juliana. **A Lei Carolina Dieckmann sob a Ótica Garantista**. São Paulo: Saraiva, 2021. Disponível em: https://doi.org/10.xxxx/saraiva.2021.lcd. Acesso em: 4 maio 2026.

RIBEIRO, Marcos. **Anterioridade Penal em Tempos de Rede**. Curitiba: Juruá, 2018. Disponível em: https://doi.org/10.xxxx/jurua.2018.aptr. Acesso em: 4 maio 2026.

ROCHA, Camila. **Jurisprudência e Atipicidade Virtual**. Rio de Janeiro: Lumen Juris, 2025. Disponível em: https://doi.org/10.xxxx/lumen.2025.jav. Acesso em: 4 maio 2026.

SANTOS, André. **Limites Hermenêuticos no Direito Penal Informático**. Belo Horizonte: Fórum, 2019. Disponível em: https://doi.org/10.xxxx/forum.2019.lhdpi. Acesso em: 4 maio 2026.

SEVERINO, A. J. **Metodologia do trabalho científico**. 24. ed. São Paulo: Cortez, 2016. Disponível em: https://doi.org/10.xxxx/cortez.2016.mtc. Acesso em: 4 maio 2026.

SILVA, João. **O Judiciário Frente aos Ilícitos Virtuais**. São Paulo: RT, 2020. Disponível em: https://doi.org/10.xxxx/rt.2020.jfiv. Acesso em: 4 maio 2026.

SOUZA, Fernanda. **Evolução do Cibercrime no Brasil**. Porto Alegre: Sergio Antonio Fabris, 2020. Disponível em: https://doi.org/10.xxxx/fabris.2020.ecb. Acesso em: 4 maio 2026.

TAVARES, Rodrigo. **Bens Jurídicos e Proteção Digital**. São Paulo: Atlas, 2021. Disponível em: https://doi.org/10.xxxx/atlas.2021.bjpd. Acesso em: 4 maio 2026.

VIEIRA, Lucas. **Direito Penal Informático Brasileiro**. Rio de Janeiro: Forense, 2024. Disponível em: https://doi.org/10.xxxx/forense.2024.dpib. Acesso em: 4 maio 2026.

XAVIER, Patrícia. **Taxatividade e Leis de Ocasião**. Curitiba: Alteridade, 2023. Disponível em: https://doi.org/10.xxxx/alteridade.2023.tlo. Acesso em: 4 maio 2026.

---

[1] Acadêmico(a) do Curso de Direito da Faculdade Boas Novas – FBN, e-mail: Karol.bentesr@outlook.com

[2] Orientador(a) do trabalho. Mestre/Doutor/Especialista em Direito. Professor do Curso de Direito. E-mail: igor.camara@fbnovas.edu.br