EFICÁCIA DAS LEIS DE COMBATE A CRIMES CIBERNÉTICOS

Lorrane Rodrigues Becalli [1], Carlos Henrique Passos Mairink[2]

Resumo: O avanço contínuo da tecnologia tem impactado diretamente o mundo jurídico, especialmente com o aumento da prática de crimes cibernéticos. O uso generalizado da internet, ampliado após a pandemia, evidenciou novos conflitos e desafios legais, principalmente no que diz respeito à coleta de provas e à identificação dos responsáveis por esses delitos. Com o aumento do acesso à internet, os crimes virtuais tornaram-se mais comuns, e muitas vezes resultam em danos pessoais e materiais. Este estudo explorou brevemente as supostas (in)eficácia e impunidade associada aos crimes cibernéticos e as dificuldades em identificar seus autores. A falta de normas específicas para punir adequadamente certas condutas no ambiente virtual agrava essa situação. O estudo teve como objetivo principal examinar a possível impunidade dos crimes cibernéticos e discutir as implicações jurídicas desse fenômeno no sistema legal brasileiro. Os objetivos específicos incluem a análise dos conceitos e da natureza jurídica dos crimes cibernéticos, a revisão da legislação e doutrina sobre o tema, e a exploração de propostas para o aprimoramento do sistema punitivo. A relevância da pesquisa se justifica pelo crescente debate sobre a punição de crimes virtuais, que representam um grave problema social no contexto digital

Palavras-chave: crimes cibernéticos; impunidade; internet; redes sociais.

Effectiveness of Laws Combating Cyber Crimes

Abstract: The continuous advancement of technology has directly impacted the legal world, especially with the rise in the practice of cyber crimes. The widespread use of the internet, which expanded after the pandemic, has highlighted new legal conflicts and challenges, particularly regarding the collection of evidence and the identification of those responsible for such offenses. With increased internet access, virtual crimes have become more common and often result in personal and material damages. This study briefly explored the alleged (in)effectiveness and impunity associated with cyber crimes, as well as the difficulties in identifying their perpetrators. The lack of specific regulations to adequately punish certain behaviors in the virtual environment exacerbates this issue. The main objective of the study was to examine the possible impunity of cyber crimes and discuss the legal implications of this phenomenon within the Brazilian legal system. Specific goals include analyzing the concepts and legal nature of cyber crimes,

[1] Discente do curso de Direito da Faculdade Minas Gerais – Famig.

[2] Revisor. Professor do curso de Direito da Faculdade Minas Gerais – Famig

reviewing relevant legislation and legal doctrine, and exploring proposals to improve the punitive system. The relevance of this research is justified by the growing debate surrounding the punishment of virtual crimes, which represent a serious social problem in the digital context.

Keywords: cybercrimes, impunity, internet, social media.

1 INTRODUÇÃO

O incessante progresso dos recursos tecnológicos e o desenvolvimento da internet têm provocado profundas repercussões no âmbito jurídico, alterando não apenas as dinâmicas processuais, mas também a forma como as relações interpessoais e institucionais se estruturam. A incorporação de novas ferramentas digitais adquiriu, especialmente no cenário pós-pandêmico, um caráter essencial para a manutenção das atividades econômicas e sociais. Entretanto, a intensa utilização dessas tecnologias também tem escancarado um aumento considerável de condutas ilícitas no ambiente virtual, evidenciando a necessidade de repensar os instrumentos jurídicos disponíveis para combatê-las.

Neste contexto, o tema central deste estudo refere-se à eficácia das leis brasileiras no combate aos crimes cibernéticos, com foco especial na (in)efetividade do ordenamento jurídico diante da crescente sofisticação das práticas criminosas digitais. O assunto, portanto, insere-se na interseção entre tecnologia, Direito Penal e Direito Processual Penal, abordando a capacidade do sistema jurídico de responder às novas demandas trazidas pela sociedade da informação. O problema de pesquisa que norteia esta investigação pode ser assim formulado: o contexto de suposta ineficácia das leis e a consequente impunidade, somadas às dificuldades de identificação dos autores, contribuem para a perpetuação dos crimes cibernéticos no Brasil? Além disso, questiona-se se os crimes virtuais estariam inseridos em uma lógica de impunidade estrutural, resultante da ausência de normas penais adequadas e da limitada eficácia prática das existentes. Como hipóteses, parte-se da premissa de que a legislação atual é insuficiente para enfrentar de forma eficaz os desafios impostos pelos crimes cibernéticos, contribuindo para a sensação de impunidade. Supõe-se ainda que a defasagem normativa e a dificuldade probatória favorecem a continuidade dessas condutas ilícitas.

O objetivo geral da pesquisa é analisar criticamente a eficácia das normas jurídicas brasileiras no enfrentamento dos crimes cibernéticos. Os objetivos específicos incluem: (i) compreender os conceitos fundamentais e a natureza jurídica dos delitos virtuais; (ii) examinar o arcabouço legislativo atual, incluindo a Lei Carolina Dieckmann (Lei nº 12.737/2012) e o Marco Civil da Internet (Lei nº 12.965/2014); (iii) investigar os principais entraves para a responsabilização dos autores desses crimes, especialmente no que tange à obtenção de provas; e (iv) discutir possíveis propostas para aprimorar a atuação estatal diante desse tipo de criminalidade. O marco teórico será composto por autores como Machado (2017), Filho (2017), Almeida e Oliveira (2022), e Bispo e Binto (2023), que discutem a crescente incidência de crimes cibernéticos no Brasil, bem como as dificuldades práticas para sua repressão. A partir de suas análises, busca-se sustentar a tese de que a legislação atual, apesar de alguns avanços, ainda carece de mecanismos eficientes e atualizados para lidar com a complexidade do ambiente digital.

Quanto à metodologia, esta pesquisa é de natureza qualitativa, com abordagem exploratória e descritiva, baseada em revisão bibliográfica e documental de artigos acadêmicos, legislações pertinentes, dados institucionais (como relatórios do Ministério Público Federal) e notícias relevantes sobre o tema. O estudo também se apoia em dados empíricos secundários, como o levantamento da Norton (2022), que aponta que 58% dos brasileiros já foram vítimas de crimes cibernéticos. Dessa forma, justifica-se a relevância deste estudo não apenas pela atualidade e gravidade do tema, mas também pela necessidade de fomentar o debate acadêmico e jurídico sobre a urgência de reformas legislativas e processuais que possam tornar o combate aos crimes cibernéticos mais eficaz, justo e proporcional. No desenvolvimento, falou-se, inicialmente, dos crimes cibernéticos e da sua adequação à legislação brasileira; em seguida, abordou-se a legislação atual e as suas lacunas; por fim, falou-se sobre a (in)eficácia e a impunibilidade dos crimes cibernéticos.

2 DESENVOLVIMENTO

2.1 Os crimes cibernéticos e a legislação brasileira

Rocha (2017, p. 13) conceitua os crimes cibernéticos, também denominados crimes virtuais, como "condutas ilícitas realizadas por meio de algum tipo de dispositivo

tecnológico, uma vez que essas ações ocorrem em um ambiente virtual". Tais delitos são perpetrados utilizando-se da internet e das tecnologias a ela associadas. Os crimes cibernéticos consistem em delitos praticados no ambiente digital, nos quais a tecnologia da informação é utilizada como principal instrumento para a execução de atos ilícitos (Maia; Costa, 2023). Essas condutas abrangem diversas atividades, que vão desde ataques a sistemas de computadores até a exploração de vulnerabilidades na internet, visando obter vantagens de ordem financeira, política ou pessoal (Maia; Costa, 2023).

De forma complementar, Lima (2012) descreve os crimes virtuais, ou cibercrimes, como quaisquer práticas ilícitas cuja execução demanda conhecimento especializado em tecnologia da informação. Assim, ambos os autores convergem ao destacar a centralidade do ambiente virtual e do domínio tecnológico como elementos distintivos desses ilícitos, ressaltando, portanto, a especificidade de sua natureza frente a outros tipos de infrações penais. Na definição de Ivette Senise Ferreira (2005), são:

> Atos dirigidos contra um sistema de informática, tendo como subespécies atos contra o computador e atos contra os dados ou programas de computador. Atos cometidos por intermédio de um sistema de informática e dentro deles incluídos infrações contra o patrimônio; as infrações contra a liberdade individual e as infrações contra a propriedade imaterial (Ferreira, 2005, p. 261).

De acordo com Corrêa, os crimes cibernéticos são caracterizados como "todos aqueles relacionados às informações arquivadas ou em trânsito por computadores, sendo esses dados acessados". Essa definição enfatiza a conexão direta entre os delitos e a manipulação de informações digitais em sistemas computacionais. Complementando essa perspectiva, Ferreira (2005) define os crimes cibernéticos como:

> Atos dirigidos contra um sistema de informática, tendo como subespécies atos contra o computador e atos contra os dados ou programas de computador. Atos cometidos por intermédio de um sistema de informática e dentro deles incluídos infrações contra o patrimônio; as infrações contra a liberdade individual e as infrações contra a propriedade imaterial (Ferreira, 2005, p. 261)

Os crimes cibernéticos, ou virtuais, configuram-se como uma categoria especializada de delitos, definida pelo meio pelo qual o ilícito é praticado, ou seja, utilizando a Rede Mundial de Computadores (Internet) ou ocorrendo em ambientes virtuais. Sob essa perspectiva, essa modalidade criminosa engloba uma ampla variedade

de tipos penais, entre os quais destacam-se a pedofilia, a clonagem de cartões de crédito, o plágio, a calúnia e a difamação, bem como o uso indevido da imagem, entre outras práticas ilícitas (Dullius; Franco; Hippler, 2012). Tais crimes evidenciam a complexidade e a diversidade dos atos ilegais associados às tecnologias digitais, ampliando os desafios para a legislação e para os mecanismos de controle e prevenção.

Assunção (2018), ao abordar o tema, elucida que essas práticas ilícitas se manifestam por meio de diversas modalidades, das quais destacam-se algumas das mais recorrentes no contexto contemporâneo. Entre elas, figuram os crimes de ódio, frequentemente representados por injúria, difamação e calúnia, as ofensas ao sentimento religioso, o bullying, os crimes que atentam contra a privacidade e a intimidade, bem como o estelionato, que constitui uma forma relevante de fraude. Essas categorias evidenciam a amplitude e a complexidade dos delitos em questão, conforme apontado pelo autor (Assunção, 2018, p. 11).

Os crimes cibernéticos podem ser classificados em três categorias principais. Primeiramente, os “crimes cibernéticos impróprios” são aqueles que podem ocorrer de forma tradicional ou por meio de computadores, sendo o dispositivo apenas um instrumento para a prática do delito. Exemplos incluem ameaça, racismo, estelionato, crimes contra a honra e falsificação de documentos, previstos no Código Penal ou em leis específicas (Queiroz, 2024). Em segundo lugar, os “crimes cibernéticos próprios” dependem exclusivamente do uso de computadores ou outros dispositivos eletrônicos com acesso à Internet, sendo o meio informático essencial para a execução do crime e para a proteção do bem jurídico (Queiroz, 2024). Exemplos incluem a invasão de dispositivos informáticos (art. 154-A) e a inserção de dados falsos em sistemas de informações (art. 313-A) (Queiroz, 2024). Por fim, existem os “crimes cibernéticos mistos”, em que a Internet é indispensável para a prática do delito, mesmo que o bem jurídico protegido não seja o sistema informático: um exemplo é a corrupção de menores via salas de bate-papo online (art. 244-B, §1° do ECA), em que o crime só ocorre por meio de dispositivos eletrônicos, mas o bem tutelado é a proteção dos direitos da criança e do adolescente (Queiroz, 2024).

A primeira previsão no ordenamento jurídico brasileiro que faz menção aos crimes praticados utilizando como intermédio um dispositivo informático surgiu com a Lei nº 9.609/98, que regula a proteção da propriedade intelectual de programas de computador e sua comercialização no País. Essa legislação foi pioneira ao tratar da proteção dos direitos autorais de programadores sobre seus softwares, assegurando diversas garantias tanto para os desenvolvedores quanto para os usuários. Além disso, estabeleceu infrações e penalidades para aqueles que, de forma ilícita, vendem, expõem à venda, introduzem no país, adquirem, ocultam ou mantêm em depósito, com fins comerciais, originais ou cópias de programas de computador produzidos em violação aos direitos autorais. Dessa forma, a Lei nº 9.609/98 desempenhou um papel fundamental no combate às práticas ilícitas relacionadas à pirataria de softwares, promovendo maior segurança jurídica no ambiente digital (Brasil, 1988). Nos artigos 12 e seguintes da Lei nº 9.609/98, são previstas as infrações e penalidades aplicáveis àqueles que violarem os direitos do autor de programas de computador, estabelecendo como sanção a detenção de seis meses a dois anos ou multa. Embora a referida lei tenha abordado crimes que poderiam ser praticados com o uso de dispositivos informáticos, seu escopo ainda era limitado a questões relacionadas diretamente ao mercado de softwares e aos profissionais que atuam nessa área. Assim, a legislação não contemplava situações mais amplas e cotidianas que passaram a surgir com o avanço e a popularização da tecnologia, deixando lacunas na proteção jurídica em outros contextos do ambiente digital.

Após a criação dessa lei, foram criadas várias outras disposições que foram incluídas no nosso ordenamento jurídico brasileiro, tendo em vista que os crimes cibernéticos estavam começando a ser praticados com mais habitualidade, e ainda era usada a interpretação infraconstitucional o que fez o legislador movimentar para criação de alguns dispositivos específicos que penalizam os crimes cometidos com o intermédio de um dispositivo informático, como:

> Art. 153, § 1° - A do Código Penal – Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública. Pena – detenção de 1 a 4 anos, e multa. Art. 313 – A do Código Penal – Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados

> corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano. Pena – reclusão, de 2 (dois) a 12 (doze) anos, e multa. Art. 313 – B do Código Penal – Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente. Pena – detenção de 3 (três) meses a 2 (dois) anos, e multa. Art. 325, § 1°, incisos I e II - Revelar fato de que tem ciência em razão do cargo e que deva permanecer em segredo, ou facilitar-lhe a revelação: Pena - detenção, de seis meses a dois anos, ou multa, se o fato não constitui crime mais grave. § 1oNas mesmas penas deste artigo incorre quem: I – permite ou facilita, mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a sistemas de informações ou banco de dados da Administração Pública; II – se utiliza, indevidamente, do acesso restrito. Art. 2°, V – Lei n.º 8.137/90 – utilizar ou divulgar programa de processamento de dados que permita ao sujeito passivo da obrigação tributária possuir informação contábil diversa daquela que é, por lei, fornecida à Fazenda Pública. Art. 72 da Lei n.º 9.504/97 – Constituem crimes, puníveis com reclusão, de cinco a dez anos: I – obter acesso a sistema de tratamento automático de dados usado pelo serviço eleitoral, a fim de alterar a apuração ou a contagem de votos; II – desenvolver ou introduzir comando, instrução, ou programa de computador capaz de destruir, apagar, eliminar, alterar, gravar ou transmitir dado, instrução ou programa ou provocar qualquer outro resultado diverso do esperado em sistema de tratamento automático de dados usados pelo serviço eleitoral; III – causar, propositadamente, dano físico ao equipamento usado na votação ou na totalização de votos ou a suas partes (Brasil, 1940).

Após esse contexto evolutivo, surgiu, na legislação brasileira, uma previsão legal específica, ainda que, como se viu a seguir, seja criticada pelas lacunas e imprecisão legal que apresenta.

2.2 Análise da legislação atual e suas lacunas

Os crimes cibernéticos permaneceram sem regulamentação legal específica até o surgimento da Lei nº 12.737, de 2012, popularmente conhecida como Lei Carolina Dieckmann (Assunção, 2018). Essa legislação foi um marco importante na proteção contra crimes cibernéticos e no estabelecimento de princípios, garantias, direitos e deveres para o uso da internet no Brasil. A Lei define a internet, no artigo 5º, inciso I, como um sistema formado pelo conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com o objetivo de viabilizar a comunicação de dados entre terminais por meio de diferentes redes (Assunção, 2018). Além disso, ela introduziu a tipificação do crime de invasão de dispositivo informático, trazendo clareza

e especificidade para a penalização desse tipo de conduta ilícita, conforme disposto no texto legal (Brasil, 2012):

O Código Penal (Decreto-Lei nº 2.848, de 7 de dezembro de 1940) passou a incluir os artigos 154-A e 154-B, tratando da invasão de dispositivos informáticos. O artigo 154-A define como crime invadir dispositivos de informática de terceiros, estejam ou não conectados à internet, por meio da violação de sistemas de segurança, com o objetivo de obter, alterar ou destruir dados sem autorização do titular, ou ainda instalar vulnerabilidades para obter vantagem ilícita (Brasil, 2012). A pena prevista é de detenção de três meses a um ano, acrescida de multa. O parágrafo primeiro estende a pena a quem criar, oferecer, distribuir, vender ou divulgar programas ou dispositivos com o objetivo de facilitar tal invasão (Brasil, 2012). O parágrafo segundo prevê aumento da pena de um sexto a um terço se houver prejuízo econômico. Já o parágrafo terceiro eleva a pena para reclusão de seis meses a dois anos e multa quando a invasão resultar na obtenção de comunicações privadas, segredos comerciais ou industriais, informações sigilosas, ou controle remoto do dispositivo, desde que não se trate de crime mais grave (Brasil, 2012). O parágrafo quarto aumenta a pena de um a dois terços caso os dados obtidos sejam divulgados, vendidos ou transmitidos a terceiros. O parágrafo quinto prevê aumento de um terço a metade da pena quando o crime for cometido contra autoridades de alto escalão, como chefes do Executivo, presidentes de tribunais, legislativos ou dirigentes da administração pública em qualquer esfera. O artigo 154-B estabelece que a ação penal para os crimes do artigo 154-A depende de representação da vítima, exceto quando o crime é praticado contra a administração pública direta ou indireta de qualquer nível de governo, ou contra empresas concessionárias de serviços públicos, situação em que a ação é de ofício (Brasil, 2012).

O Art. 154-A do Código Penal, conforme analisado por Cabette (2013), apresenta uma formulação que pode gerar interpretações confusas, especialmente no que se refere à exigência de "violação indevida de mecanismo de segurança". Segundo o autor, essa redação não apenas demanda a existência de mecanismos de segurança instalados no dispositivo invadido, mas também que esses mecanismos estejam efetivamente ativos no momento da invasão. Caso contrário, mesmo diante de uma intrusão não autorizada, o fato seria considerado atípico, o que compromete a aplicação prática da

norma (Almeida, 2022). Cabette (2013) exemplifica essa problemática ao imaginar um cenário em que um computador, normalmente protegido por um antivírus, tem esse sistema de segurança desativado temporariamente pelo próprio proprietário. Em situações como essa, a invasão do dispositivo, ainda que claramente indevida, não configuraria um crime, devido à ausência de violação ativa de um mecanismo de segurança no instante do ataque. Essa interpretação, segundo ele, é comparável à ideia de que uma casa com portas abertas permitiria a entrada de qualquer pessoa sem a autorização do morador — uma lógica que claramente não se aplica no direito penal tradicional, mas que, de forma equivocada, parece ter sido adotada no contexto da proteção dos sistemas informáticos (Cabette, 2013).

Na prática, essa redação legal impacta diretamente a efetividade da norma, uma vez que limita a abrangência da criminalização de invasões a dispositivos informáticos e deixa lacunas que podem ser exploradas. A exigência de mecanismos de segurança ativos no momento da invasão torna mais difícil a tipificação do crime, enfraquecendo a proteção jurídica aos sistemas informáticos e gerando insegurança sobre a aplicação da lei. Isso reflete, conforme apontado por Cabette, um erro de raciocínio legislativo, que não considerou adequadamente a complexidade das situações práticas envolvendo invasões cibernéticas. A Lei 12.737/12, assim, trouxe modificações significativas ao Código Penal ao acrescentar parágrafos nos artigos 266, que trata da “Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública”, e 298, que versa sobre a “Falsificação de documento particular” (Lima, 2012).

Posteriormente, em 2014, foi sancionada a Lei 12.965, amplamente conhecida como o “Marco Civil da Internet”. Essa legislação surgiu com o propósito central de preencher lacunas existentes no ordenamento jurídico no que se refere aos crimes praticados no ambiente virtual, estabelecendo princípios fundamentais, como a inviolabilidade da intimidade e da vida privada, o sigilo e a proteção do fluxo de comunicações realizadas pela internet, além de definir garantias, direitos e deveres para o uso responsável da internet no Brasil (Brasil, 2014).

A evolução da legislação brasileira em relação aos crimes cibernéticos evidencia avanços significativos, abrangendo desde a proteção inicial da propriedade intelectual de programas de computador até a formulação de leis específicas, como a Lei Carolina Dieckmann e o Marco Civil da Internet. Embora essas normas tenham contribuído para ampliar a clareza e estabelecer punições mais rigorosas para infrações cometidas no ambiente virtual, persistem desafios na aplicação eficaz dessas legislações, especialmente no que diz respeito à identificação dos responsáveis pelos crimes e à complexidade crescente das infrações digitais. Dessa forma, a legislação brasileira continua em constante adaptação para acompanhar a sofisticação cada vez maior das atividades criminosas no espaço cibernético.

2.3 A (in)eficácia e a impunibilidade dos crimes cibernéticos

A Lei nº 12.737 de 2012, como mencionado, representou um avanço relevante no tocante à criminalização de práticas ilícitas no ambiente virtual e por meio de dispositivos tecnológicos. Como destacado por Almeida e Oliveira (2022), é inegável que a inserção de normas relativas à questão, ainda que de forma tímida, representam avanço em relação ao contexto anterior, de total imprevisibilidade. Contudo, conforme argumentam Tabet, Pereira e Jorge (2016, p. 276), ao se observar o amplo espectro das práticas criminosas que podem ser realizadas através da internet e no ambiente virtual, verifica-se um aumento expressivo da criminalidade digital, o que pode ser um indicativo da inadequação ou da insuficiência das disposições legais. Há de se recorda, inclusive, como estabelecido por Cabette (2013), que parte da doutrina, ao contrário do que parece ser o entendimento jurisprudencial, entende pela inadequação da lei de 2012, dadas as suas lacunas e imprecisões, o que interfere diretamente na tutela jurídica (e judicial) prestada sobre esses casos e, indiretamente, à efetividade da proposta legislativa. Esse cenário faz com que a legislação brasileira, apesar dos progressos, pareça desatualizada e incapaz de estabelecer um sistema jurídico robusto que efetivamente reprima e previna tais delitos. Ainda que a jurisprudência tenha demonstrado uma tendência favorável à responsabilização e condenação de indivíduos que praticam crimes pela internet, as lacunas existentes na legislação continuam a permitir que certos criminosos escapem de punições adequadas (Tabet; Pereira; Jorge, 2016, p. 276). Conforme destacam Bispo e Binto (2023, p. 355), os esforços para

combater os crimes virtuais no Brasil têm se mostrado pouco eficazes, considerando que "(...) crimes virtuais continuam a ocorrer diariamente e, com o avanço tecnológico, as agências responsáveis pela aplicação da lei não estão sendo eficientes para reprimir os infratores". As autoras apontam que, apesar dos avanços obtidos, a legislação brasileira voltada para os crimes cibernéticos ainda apresenta lacunas importantes, especialmente no que tange à aplicação de punições adequadas e à produção eficaz de provas para embasar os processos judiciais.

Embora a lei tenha trazido alterações ao Código Penal, ainda persiste uma notável falta de clareza quanto à definição de termos técnicos fundamentais, o que compromete a aplicação efetiva dos tipos penais nela previstos. Um exemplo evidente é o crime de invasão de sistemas informáticos, cuja tipificação exige que a invasão seja realizada à força, mas falha em detalhar com precisão quais mecanismos de segurança devem ser violados para configurar o crime. Essa falta de especificidade acaba por abrir margem para interpretações divergentes, resultando, em muitos casos, na impunidade de infratores que acessam sistemas sem autorização, mas sem violar de forma inequívoca os mecanismos de proteção estipulados (Bispo; Binto, 2023, p. 362). Além disso, no que tange ao tempo mínimo de aplicação das penas, frequentemente inferior a um ano, verifica-se que essas punições são classificadas como de menor potencial ofensivo, conforme estabelecido pela Lei 9.099/95. Essa qualificação permite a suspensão condicional do processo, desde que o autor do delito não possua condenações anteriores. Essa abordagem jurídica tende a minimizar a gravidade das ações cometidas, comprometendo a eficácia do sistema penal em coibir comportamentos criminosos. A incapacidade de impor sanções mais severas para crimes cibernéticos figura entre as críticas mais contundentes, uma vez que as penas aplicáveis ao acesso não autorizado a informações e às atividades de hackers são amplamente consideradas brandas e insuficientes para desestimular futuras infrações (Bispo; Binto, 2023, p. 363).

As penalidades, que variam de três meses a um ano de prisão, não correspondem à seriedade dos prejuízos que tais crimes podem causar, muitas vezes com implicações financeiras, sociais e institucionais graves. Além disso, é crucial que esses crimes sejam julgados com celeridade, dado que a pena mínima aumenta o risco de prescrição,

culminando na impunidade dos infratores. Essa conjuntura, conforme destacam as autoras, reforça a necessidade urgente de revisar as penalidades e a abordagem do sistema jurídico em relação aos crimes cibernéticos, de modo a assegurar que as consequências legais sejam proporcionais à gravidade das ações praticadas, promovendo, assim, maior eficácia na prevenção e repressão dessas infrações (Bispo; Binto, 2023, p. 363).

Especificamente no que se refere às penas, até a promulgação da Lei nº 14.155 de 2021, o artigo 154-A do Código Penal estabelecia que o crime de invasão de dispositivo informático descrito no caput era punível com pena de detenção de 03 (três) meses a 01 (um) ano, além de multa. Nos casos em que a invasão resultasse em prejuízo econômico, a pena poderia ser majorada de um sexto a um terço (§2º) (Brasil, 2012). Além disso, se a invasão resultasse na obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas ou controle remoto não autorizado do dispositivo invadido, a pena prevista era de 06 (seis) meses a 02 (dois) anos de detenção, e multa, salvo se a conduta configurasse crime mais grave (§3º). Essa pena poderia ainda ser ampliada de um a dois terços, caso os dados ou informações obtidas fossem divulgados, comercializados ou transmitidos a terceiros, independentemente do título sob o qual isso ocorresse (§4º) (Brasil, 2012).

Além disso, a legislação previa o aumento da pena de um terço à metade quando o crime fosse praticado contra autoridades como o Presidente da República, governadores e prefeitos; o Presidente do Supremo Tribunal Federal (STF); o Presidente da Câmara dos Deputados, do Senado Federal, de Assembleias Legislativas de Estados, da Câmara Legislativa do Distrito Federal ou de Câmaras Municipais; ou ainda contra o dirigente máximo da administração direta e indireta das esferas federal, estadual, municipal ou do Distrito Federal (§5º e incisos) (BRASIL, 2012). Mais recentemente, a Lei nº 14.155 de 2021 foi sancionada, introduzindo alterações significativas no Código Penal e no Código de Processo Penal, revisando as disposições relacionadas aos crimes virtuais, com o objetivo de atualizar e ampliar o alcance das normas para enfrentar os desafios impostos pela evolução tecnológica. No caso das alterações relativas ao Código Penal:

> Art. 1º O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), passa a vigorar com as seguintes alterações:"Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita:Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa. (...) § 2º Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico. (...) Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa. (...) "Art. 155. (...) § 4º-B. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo. § 4º-C. A pena prevista no § 4º-B deste artigo, considerada a relevância do resultado gravoso: I – aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional; II – aumenta-se de 1/3 (um terço) ao dobro, se o crime é praticado contra idoso ou vulnerável (...) Art. 171. (...) Fraude eletrônica § 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo. § 2º-B. A pena prevista no § 2º-A deste artigo, considerada a relevância do resultado gravoso, aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional (...). Estelionato contra idoso ou vulnerável § 4º A pena aumenta-se de 1/3 (um terço) ao dobro, se o crime é cometido contra idoso ou vulnerável, considerada a relevância do resultado gravoso (Brasil, 2021).

Pode-se observar que as penas atribuídas aos ilícitos cibernéticos foram ampliadas em alterações legislativas recentes. Durante a vigência da norma introduzida pela Lei de 2012, as penas eram frequentemente criticadas pela doutrina como "brandas", demonstrando uma tendência a não reprimir adequadamente e, em alguns casos, até a estimular a prática de crimes virtuais, como será evidenciado nos resultados da pesquisa. Embora a atualização legal tenha representado um avanço, ainda persiste o debate sobre a (im)punibilidade desses delitos, reforçando a necessidade de normas mais detalhadas e específicas que abordem as particularidades dos crimes cibernéticos de maneira eficaz e abrangente. A legislação, ainda que abrangente em alguns aspectos, demonstra limitações significativas frente à rápida evolução tecnológica e às sofisticadas estratégias empregadas na cibercriminalidade.

O Brasil, apesar de ser um dos países com maior uso da Internet, ainda não possui uma norma penal específica e unificada que abarque todos os crimes cibernéticos (Queiroz, 2024). A recente adesão à Convenção de Budapeste busca suprir essa lacuna, oferecendo maior proteção aos usuários, ferramentas forenses, cooperação internacional e capacitação das autoridades responsáveis pela investigação (Queiroz, 2024). No entanto, as penas atuais, previstas no Código Penal e em legislações esparsas, são consideradas leves e pouco eficazes como fator de dissuasão, o que permite que criminosos continuem repetindo suas condutas sem receio de sanções mais severas (Queiroz, 2024).

A dificuldade em identificar e responsabilizar os autores de crimes virtuais, especialmente aqueles que operam de forma anônima ou utilizando servidores localizados fora do país, expõe a inadequação de determinados dispositivos legais em acompanhar a complexidade e o dinamismo do ambiente digital. Além disso, embora o aumento das penas represente um avanço, ele não supre a urgente necessidade de aprimoramento técnico das autoridades investigativas, que frequentemente enfrentam desafios decorrentes da falta de recursos adequados para rastrear atividades criminosas e coletar provas digitais de maneira eficaz. Essa lacuna técnica, aliada à crescente sofisticação dos delitos virtuais, evidencia a necessidade de uma revisão estrutural tanto no arcabouço legal quanto nas ferramentas disponíveis para as investigações cibernéticas.

> Em resposta a estas inadequações, numerosos especialistas e defensores dos direitos cibernéticos afirmam que é necessária uma abordagem unida dos legisladores, das agências responsáveis pela aplicação da lei e do campo tecnológico. Isto exige o estabelecimento de legislação mais robusta, a sensibilização, a garantia de recursos suficientes para investigações, a defesa da colaboração internacional e, o mais importante, a educação dos indivíduos sobre a segurança digital e o reconhecimento da atividade criminosa (Bispo; Binto, 2023, p. 363).

Diante de todas essas considerações, é imprescindível que a legislação brasileira evolua continuamente, ajustando-se às inovações tecnológicas e às novas práticas delitivas que emergem no ambiente virtual. A criação de um sistema jurídico capaz de responder de maneira eficaz às atividades criminosas realizadas por meio da internet e em ambientes virtuais torna-se essencial para assegurar a proteção real dos usuários e

a responsabilização adequada dos infratores. Além disso, é fundamental que a legislação brasileira amplie seu alcance para abranger integralmente os diversos delitos que podem ser praticados nesse contexto, estabelecendo mecanismos claros e eficazes para prevenção, repressão e penalização dessas condutas. Esse processo de evolução legislativa deve ser acompanhado de iniciativas que fortaleçam as capacidades investigativas e de fiscalização, promovendo um ambiente digital, sobretudo, mais seguro.

3 CONCLUSÕES

Ao longo deste estudo, foi possível constatar que, embora a legislação brasileira tenha avançado na criminalização de práticas ilícitas cometidas no ambiente digital — com marcos importantes como a Lei nº 12.737/2012 (Lei Carolina Dieckmann) e o Marco Civil da Internet —, esses avanços ainda se mostram insuficientes diante da crescente complexidade e sofisticação dos crimes cibernéticos. No primeiro capítulo, ao abordar os conceitos fundamentais e a natureza jurídica desses delitos, evidenciou-se que a própria definição de crimes virtuais permanece imprecisa, o que dificulta sua identificação e responsabilização. Em seguida, ao analisar o arcabouço normativo vigente, foram identificadas lacunas significativas, especialmente no que tange à tipificação clara de condutas e à adequação das penas aplicáveis. Por fim, ao discutir a (in)eficácia e a impunidade estrutural desses crimes, verificou-se que as dificuldades probatórias e a morosidade na investigação reforçam a percepção de que o sistema jurídico não está preparado para enfrentá-los adequadamente.

O problema de pesquisa, que questiona se a suposta ineficácia das leis brasileiras e a dificuldade de identificação dos autores contribuem para a perpetuação dos crimes cibernéticos, foi respondido afirmativamente. Constatou-se que, de fato, a combinação entre normas desatualizadas, penas brandas e obstáculos técnicos na produção de provas alimenta um cenário de impunidade. Essa conclusão é reforçada por dados como o da pesquisa realizada pela Norton (2022), que revelou que 58% dos brasileiros já foram vítimas de crimes virtuais, o que demonstra a gravidade e a extensão do problema. Nesse sentido, confirma-se a hipótese de que a legislação atual não é suficiente para coibir de forma eficaz os delitos cibernéticos, sendo necessária uma reforma legislativa

mais profunda. As recentes alterações que aumentaram penas são um passo positivo, mas não resolvem as ambiguidades legais e os entraves processuais enfrentados na prática. Além disso, a limitação técnica das instituições de persecução penal, aliada à atuação muitas vezes anônima dos infratores e ao uso de servidores internacionais, impõe desafios adicionais à repressão e punição eficaz desses crimes.

Portanto, torna-se imprescindível que o enfrentamento da criminalidade digital no Brasil seja estruturado a partir de um tripé: (i) revisão normativa — com o aprimoramento de dispositivos como o art. 154-A do Código Penal, eliminando ambiguidades e ampliando a proteção jurídica frente às novas modalidades de invasão e fraude digital; (ii) formação e capacitação especializada — para que agentes da lei, Ministério Público e Judiciário estejam tecnicamente preparados para lidar com crimes digitais de alta complexidade; e (iii) criação de um órgão especializado, como uma agência nacional de combate aos crimes cibernéticos, capaz de centralizar informações, coordenar esforços e atuar em parceria com instituições nacionais e internacionais. Conclui-se, assim, que o fortalecimento do aparato jurídico e institucional, aliado à constante atualização tecnológica, é condição essencial para que o Brasil possa enfrentar de maneira eficaz os desafios impostos pela criminalidade no ambiente virtual e superar a atual lógica de impunidade estrutural que favorece a continuidade dessas condutas ilícitas.

REFERÊNCIAS

ALMEIDA, Haian de Assis Lopes; OLIVEIRA, Tamar Ramos de. **Crimes virtuais: o avanço dos crimes eletrônicos e a evolução das leis específicas no Brasil.** Revista Ibero-Americana de Humanidades, Ciências e Educação. São Paulo, v.8, n.11, nov. 2022.

ASSUNÇÃO, A. A. S. **Crimes virtuais**. Dissertação (apresentada à UniEvangélica). Unievangélica, Anápolis, 2018.

BISPO, Adrielle da Silva; BINTO, Emanuel Vieira. **Crimes cibernéticos: da ineficácia da Lei Carolina Dieckmann na prática de crimes virtuais**. Revista Ibero-Americana De Humanidades, Ciências E Educação, 9(11), 354–369, nov. 2023.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília: Senado, 1988.

BRASIL. **Decreto-Lei nº 2.848 de 07 de dezembro de 1940**. Institui o Código Penal. Diário Oficial da União: Rio de Janeiro, 1940. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848.htm>. Acesso em: 18 jun. 2025.

BRASIL. **Decreto-Lei nº 3.689 de 03 de outubro de 1941**. Institui o Código de Processo Penal. Diário Oficial da União: Rio de Janeiro, 1941. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689.htm>. Acesso em: 18 jun. 2025.

BRASIL. **Lei nº 8.069 de 13 de julho de 1990**. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Diário Oficial da União, Brasília, 16 jul. 1990. Disponível em: < http://www.planalto.gov.br/Ccivil_03/leis/L8069.htm>. Acesso em: 18 jun. 2025.

BRASIL. **Lei nº 10.406 de 2002**. Institui o Código Civil. Diário Oficial da União, Brasília, 11 jan. 2002.

BRASIL. **Lei nº 12.735 de 30 de novembro de 2012**. Altera o Código Penal para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticados contra sistemas informatizados e similares. Diário Oficial da União, Brasília, 2012. Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm>. Acesso em: 18 jun. 2025.

BRASIL. **Lei nº 12.737 de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos. Diário Oficial da União, Brasília, 2012. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 18 jun. 2025.

BRASIL. **Lei nº 12.965 de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União, Brasília, 2014 [S.L]: 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 18 jun. 2025.

BRASIL. Ministério Público Federal. **Roteiro de atuação sobre crimes cibernéticos.** Portal do Ministério Público Federal, Brasília, 2013.

CABETTE, Eduardo Luís Santos. **O novo crime de invasão de dispositivo informático**. Portal ConJur, São Paulo, 04 fev. 2013. Disponível em: <http://www.conjur.com.br/2013-fev-04/eduardo-cabette-crime-invasao-dispositivo-informatico>. Acesso em: 18 jun. 2025.

DULLIUS, Aladio Anastacio; FRANCO, Elisa Lunardi; HIPPLER, Aldair. **Dos crimes praticados em ambientes virtuais**. [S.L.]: 2012. Disponível em: < http://www.conteudojuridico.com.br/artigo,dos-crimes-praticados-em-ambientes-virtuais,38483.html>. Acesso em: 04 jul. 2025.

FERREIRA, Ivette Senise. **Direito e internet: aspectos jurídicos relevantes**. 2 ed. São Paulo: Editora Quartier Latin, 2005.

LIMA, Simão Prado. **Crimes virtuais: uma análise da eficácia da legislação brasileira e o desafio do direito penal na atualidade**. Sergipe, 2012. Disponível em: <

http://www.ambitojuridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=15260&revista_caderno=3>. Acesso em: 04 jul. 2025.

MAIA, Karolline Barbosa; COSTA, Cezar Henrique Ferreira. **Crimes Cibernéticos**. Revista Ibero-Americana de Humanidades, Ciências e Educação, [S. l.], v. 9, n. 10, p. 109–126, 2023. DOI: 10.51891/rease.v9i10.11580. Disponível em: https://periodicorease.pro.br/rease/article/view/11580. Acesso em: 7 nov. 2025.

PANCINI, Laura. **58% dos brasileiros sofreram crimes cibernéticos, aponta estudo da Norton.** Portal da Revista Exame, 11 mar. 2022. Disponível em: https://exame.com/tecnologia/58-dos-brasileiros-sofreram-crimes-ciberneticos-aponta-estudo-da-norton/. Acesso em: 18 jun. 2025.

QUEIROZ, Liv Ferreira Augusto Severo. **Os crimes cibernéticos no ordenamento jurídico brasileiro: investigação criminal e desafios.** Revista do CNMP, 12. ed., 2024.

ROCHA, A. A. **Cibercriminalidade: os crimes cibernéticos e os limites da**

liberdade de expressão na internet. Monografia (apresentada ao curso de bacharelado em Direito da Faculdade de Ensino Superior e Formação Integral). Faculdade de Ensino Superior e Formação Integral, São Paulo, 2017

TABET, Arthur Gomes; PEREIRA, Luiza Barbosa; JORGE, Ricardo Clemente. **Uma análise da ineficácia do direito penal brasileiro em relação à internet**. Jornal Eletrônico Faculdades Integradas Vianna Júnior, Ano VIII, dez. 2016.