e-ISSN 2178-4396

CIBERCRIME E A DESATUALIZAÇÃO DA LEGISLAÇÃO PENAL

Cybercrime and the outdated of criminal legislation

Thauany Lins Bezerra[1]
Karine Cordazzo[2]

RESUMO

O avanço tecnológico e a proliferação de crimes no ambiente virtual impõem um desafio crítico ao sistema penal brasileiro. Este artigo analisa a desatualização do Código Penal (CP) e do Código de Processo Penal (CPP) diante da complexidade dos cibercrimes (incluindo fraudes *online*, invasão de sistemas e crimes contra a honra digital). O estudo demonstra que a lacuna normativa e a dificuldade de subsunção típica resultam, frequentemente, na atipicidade da conduta, comprometendo o princípio da legalidade e a efetividade da sanção penal. A partir de uma análise bibliográfica e legal-crítica, o trabalho conclui pela urgência da modernização legislativa, propondo diretrizes para a criação de normas mais flexíveis e perenes, capazes de acompanhar a dinâmica digital e garantir a punição efetiva dos infratores, essenciais para a segurança pública e a confiança na nação digital

Palavras-chave: cibercrime; crimes virtuais; atualização legislativa; fraude online; responsabilidade penal digital.

ABSTRACT

Technological advances and the proliferation of crimes in the virtual environment pose a critical challenge to the Brazilian criminal justice system. This article analyzes the outdated nature of the Penal Code (CP) and the Code of Criminal Procedure (CPP) in light of the complexity of cybercrimes (including online fraud, system intrusion, and crimes against digital reputation). The study demonstrates that the regulatory gap and the difficulty of typical subsumption often result in atypical conduct, compromising the principle of legality and the effectiveness of criminal sanctions. Based on a bibliographic and legal-critical analysis, the study concludes that legislative modernization is urgently needed, proposing guidelines for the creation of more flexible and enduring norms capable of keeping pace with digital dynamics and ensuring the effective punishment of offenders, which is essential for public safety and trust in the digital nation.

Keywords: *cybercrime; virtual crimes; legislative update; online fraud; digital criminal liability.*

1 Discente do Curso de Direito do Centro Universitário da Grande Dourados – UNIGRAN. ORCID: 0009-0009-2208-2389. E-mail: 011.6614@alunos.unigran.br.

2 Doutora em Direito pela Instituição Toledo de Ensino (ITE). Mestra em Fronteiras e Direitos Humanos pela Universidade Federal da Grande Dourados (UFGD). Docente no curso de Direito do Centro Universitário da Grande Dourados. ORCID: 0000-0003-3465-0792. E-mail: karine.cordazzo@unigran.br.

1 INTRODUÇÃO

Com o avanço acelerado das tecnologias da informação e comunicação, a sociedade vivencia uma transformação digital sem precedentes, impactando profundamente as relações pessoais, profissionais e jurídicas. No entanto, esse processo, ao mesmo tempo em que proporciona inúmeros benefícios, também dá margem ao surgimento de novas formas de criminalidade, que exploram as fragilidades do ambiente virtual. Nesse contexto, os crimes cibernéticos ganham cada vez mais espaço, tornando-se uma ameaça real e constante à segurança digital dos indivíduos, instituições e até mesmo do Estado.

A popularização da internet e o fácil acesso às tecnologias digitais ampliaram significativamente o número de usuários, mas também evidenciaram um grave problema social: o analfabetismo digital. Pessoas em situação de vulnerabilidade tornam-se alvos frequentes de golpes virtuais, fraudes e invasões de privacidade, muitas vezes sem compreenderem o funcionamento básico dos meios digitais ou os riscos a que estão expostas. O desconhecimento contribui para o aumento da criminalidade e dificulta a prevenção e o combate eficaz a essas condutas ilícitas.

A legislação penal brasileira, historicamente voltada à repressão de condutas típicas do mundo físico, revela-se insuficiente diante da complexidade e da velocidade com que os delitos digitais se desenvolvem. A ausência de tipificações específicas, aliada à dificuldade de aplicação prática das normas existentes, contribui para a sensação de impunidade e para o crescimento exponencial dessas infrações. Tal cenário exige uma reflexão crítica sobre a necessidade de atualização do ordenamento jurídico, com vistas à efetiva responsabilização dos infratores e à proteção dos bens jurídicos vulneráveis no ciberespaço.

Nesse sentido, este artigo tem como objetivo analisar a evolução dos crimes cibernéticos e a resposta normativa oferecida pelo Direito Penal brasileiro, destacando os principais marcos legislativos, as lacunas ainda existentes e os desafios enfrentados pelos operadores do Direito. A pesquisa, de natureza qualitativa e exploratória, adota o método de procedimento bibliográfico e documental. A fundamentação teórica se baseia em doutrinas jurídicas, na análise da legislação (incluindo as recentes alterações no Código Penal e Processual Penal) e em jurisprudências relevantes do Superior Tribunal de Justiça (STJ) e do Supremo Tribunal Federal (STF). Específicas, jurisprudências e dados oficiais. Busca-se, assim, contribuir de forma crítica para o debate sobre a urgência de uma reforma penal estrutural que contemple as especificidades do ambiente digital, promovendo maior segurança jurídica e eficácia na persecução penal dos delitos virtuais.

2 O SURGIMENTO DO CRIME VIRTUAL

Para que este assunto seja compreendido com clareza, é necessário identificar o marco inicial e compreender de onde vieram as expressões criativas e as nomenclaturas utilizadas para definir eventos catastróficos no universo digital. Vale destacar que há divergências doutrinárias quanto ao primeiro delito informático registrado.

Jesus e Milagres (2016) afirmam que para alguns estudiosos, o primeiro crime cibernético teria ocorrido no *Massachusetts Institute of Technology* (MIT), em 1964, quando um estudante de 18 anos cometeu um ato classificado como cibercrime e foi advertido pelos superiores. Enquanto isso, outros autores apontam como primeiro caso de hacking o episódio ocorrido em 1978, na Universidade de Oxford, quando um estudante invadiu uma rede de computadores e copiou uma prova. Na época, os Estados Unidos ainda não possuíam legislação específica sobre crimes informáticos. A Flórida foi o primeiro estado americano a instituir leis sobre informática, também em 1978.

Segundo Schjolberg (2008), muitas pessoas se engajaram no combate ao crime eletrônico desde os primórdios. Dentre elas, destaca-se o americano Donn B. Parker, considerado um dos primeiros pesquisadores do cibercrime, atuando como consultor de segurança no Stanford Research Institute. Ele foi o autor do manual *Computer Crime – Criminal Justice Resource Manual*, desenvolvido em 1979, considerado uma "enciclopédia" para autoridades, inclusive de fora dos Estados Unidos.

A primeira iniciativa internacional significativa sobre cibercrime foi a Conferência sobre Aspectos Criminológicos do Crime Econômico, realizada em 1976, no âmbito do Conselho da Europa, em Estrasburgo. No entanto, foi somente na década de 1990 que os crimes cibernéticos passaram a se proliferar em maior escala(Jesus; Milagres, 2016).

Durante a década de 1980, John Draper, conhecido como *Captain Crunch*, ficou famoso por ter inventado o *phreaking*, técnica que utilizava um apito capaz de emitir o tom de 2.600 Hz, enganando o sistema telefônico americano e permitindo a realização de ligações gratuitas(Jesus; Milagres, 2016).

As condutas mais comuns nessa época envolviam a disseminação de vírus, pornografia infantil, invasão de sistemas e pirataria digital, iniciando-se, assim, uma maior conscientização sobre a importância da segurança cibernética.

Em 1988, Robert Morris criou um dos primeiros vírus de computador do mundo, que afetou cerca de seis mil computadores. Foi o primeiro *hacker* condenado sob a então recente *Computer Fraud and Abuse Act* dos Estados Unidos(Jesus; Milagres, 2016).

Em 1990, Kevin Mitnick invadiu redes de operadoras de telefonia e provedores de internet norte-americanos. Preso em 1995, cumpriu cinco anos de detenção. No mesmo ano, Kevin Poulsen interceptou chamadas telefônicas de uma rádio da Califórnia e, ao se

tornar o 102º ouvinte, ganhou um carro Porsche. Ele foi preso por quatro anos e atualmente é diretor do site *Security Focus*. Desde então, casos de *hacking* têm se tornado cada vez mais frequentes ao redor do mundo (Jesus; Milagres, 2016).

No Brasil, os primeiros registros de crimes de *phishing scam* bancário (roubo de senhas) surgiram em 1999. Outro caso marcante envolveu um empresário e ex-controlador de uma rede de varejo, acusado de enviar, de Londres, e-mails com informações falsas ao mercado financeiro, gerando alarme sobre uma suposta falência bancária(Jesus; Milagres, 2016).

Em 1996, Ivan Lira de Carvalho foi questionado se a internet representaria apenas um novo meio para a execução de crimes antigos ou se daria origem a novos delitos. Ele esclareceu que ambas as possibilidades coexistem, pois, embora crimes tradicionais sejam praticados por meio da internet, surgem também novos crimes atrelados ao avanço tecnológico (Carvalho, 1996).

O autor ressaltou que, embora o processo legislativo seja mais lento que a evolução tecnológica, os operadores do Direito não devem se limitar à espera de novas leis. Caso a conduta criminosa se enquadre nas normas vigentes, o aplicador da lei deve agir, mesmo diante da ausência de atualizações legislativas (Carvalho, 1996).

Segundo Damásio de Jesus e José Antônio Milagres (2016), em outubro de 2000, o ex-Prefeito Paulo Maluf tornou-se o primeiro político brasileiro vítima de sabotagem digital durante as eleições.

Em novembro de 2002, o Brasil passou a ser considerado o maior "exportador" de criminalidade via internet. A primeira condenação de um pirata virtual no país ocorreu apenas em janeiro de 2004: um jovem de 19 anos foi sentenciado a seis anos e quatro meses de prisão por aplicar golpes pela internet no Brasil e nos Estados Unidos(Jesus; Milagres, 2016).

De acordo com dados da Polícia Federal em 2004, de cada dez hackers ativos no mundo, oito residiam no Brasil. Além disso, dois terços das páginas de pedofilia na internet, identificadas por investigações brasileiras e estrangeiras, tinham origem no país. A Polícia Federal declarou ainda, à época, que o crime informático já gerava mais lucros do que o tráfico de drogas. Dados do Colégio Notarial do Brasil (CNB) indicam que o número de crimes virtuais no país aumentou 70% entre 2012 e 2013 (Kurtz, 2014).

No segundo semestre de 2022, a maioria dos incidentes cibernéticos foi motivada por interesses financeiros, sendo a espionagem o segundo principal fator (Neotel, 2023). Nessa tessitura, oFortiGuard Labs utiliza a estrutura MITRE ATT&CK para classificar as táticas, técnicas e procedimentos utilizados por agentes mal-intencionados, descrevendo como eles exploram vulnerabilidades.

3 EVOLUÇÃO DOS CRIMES CIBERNÉTICOS E DA LEGISLAÇÃO PENAL INFORMÁTICA

A criação das Leis n. 12.735/2012 e n. 12.737/2012 representou um grande avanço no combate aos crimes virtuais, haja vista que os dispositivos legais criaram tipos penais incriminadores, mediante a inclusão dos artigos 154-A e 154-B no Código Penal, *in verbis*:

> 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:
>
> […]
>
> Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos (Brasil, 1940).

A consolidação das legislações voltadas à repressão de condutas ilícitas praticadas em meio digital representa um avanço importante no ordenamento jurídico brasileiro. Nesse contexto, destaca-se a Lei n. 12.737/2012, conhecida como "Lei Carolina Dieckmann", que introduziu tipos penais específicos relacionados à invasão de dispositivos informáticos. Essa norma é reconhecida como o primeiro instrumento legislativo com o propósito claro de proteger juridicamente bens no ambiente virtual, constituindo-se como um marco regulatório voltado à realidade digital (Brasil, 2012).

Apesar disso, autores como Cardoso (2017) argumentam que, embora inovadora, a referida lei promoveu alterações pontuais e não suficientemente robustas para enfrentar os desafios complexos que o Direito encontra diante da cibernética contemporânea.

Ainda que representem avanços iniciais na seara penal, tais dispositivos legais não são, por si sós, capazes de conter de forma eficaz a crescente incidência de delitos virtuais. Sua importância reside, sobretudo, no simbolismo de uma resposta estatal à demanda social por proteção jurídica no meio digital, funcionando como ponto de partida para a construção de um arcabouço normativo mais sólido.

Mais recentemente, o legislador buscou ampliar essa tutela por meio da Lei n. 14.155/2021, sancionada em 28 de maio de 2021, a qual promoveu significativas alterações no Código Penal e no Código de Processo Penal. Essa norma ampliou a tipificação de crimes como a invasão de dispositivo informático, furto mediante fraude eletrônica e estelionato digital, além de ajustar penalidades e procedimentos processuais a fim de tornar

mais efetiva a persecução penal desses delitos (Maranhão, 2022).

Nesse cenário, os crimes cometidos no ambiente virtual eram inicialmente tratados como crimes-meio, ou seja, infrações em que o meio digital era apenas o instrumento utilizado para a consumação do ato ilícito. Sobre isso, Pinheiro (2014, p. 307) ressalta:

> Não é um crime-fim por natureza, ou seja, o crime cuja modalidade só ocorre em ambiente virtual, á exceção dos crimes cometidos por hackers, que de algum modo podem ser enquadrados na categoria de estelionato, extorsão, falsidade ideológica, fraude, entre outros.

Apenas para fins pedagógicos, a classificação de crime-meio é utilizada para descrever aquelas infrações em que o meio digital atua apenas como um instrumento para a prática de delitos já conhecidos, como estelionato, extorsão ou falsidade ideológica. Nesses casos, a internet ou qualquer tecnologia não é o objeto do crime, mas sim o canal pelo qual ele se concretiza.

Essa distinção é útil para a análise jurídica e para a definição das estratégias de enfrentamento. Inclusive, no âmbito do princípio da consunção, que regula o conflito aparente de normas penais (Masson, 2019), o Superior Tribunal de Justiça já entendeu que, se um crime-meio for cometido com a finalidade exclusiva de viabilizar um crime-fim, a extinção da punibilidade deste último alcança também aquele:

> No caso em que a falsidade ideológica tenha sido praticada com o fim exclusivo de proporcionar a realização do crime de descaminho, a extinção da punibilidade quanto a este – diante do pagamento do tributo devido – impede que, em razão daquela primeira conduta, considerada de forma autônoma, proceda-se à persecução penal do agente. Isso porque, nesse contexto, exaurindo-se o crime-meio na prática do crime-fim, cuja punibilidade não mais persista, falta justa causa para a persecução pelo crime de falso, porquanto carente de autonomia.

Assim, embora algumas condutas criminosas se utilizem da internet apenas como ferramenta, outras já nascem e se desenvolvem exclusivamente no espaço digital, exigindo uma resposta jurídica cada vez mais especializada e adaptada à complexidade desses fenômenos. Ademais, não apenas *hackers* podem praticar crimes-fim informáticos, mas qualquer pessoa (Jesus; Milagres, 2016).

Conforme verificado por Damásio de Jesus e José Antônio Milagres (2016), não há consenso quanto ao perfil do criminoso digital, embora existam relevantes estudos e pesquisas sobre o tema. Na maioria dos casos, os crimes não são de "alta tecnologia". Costuma-se associar o crime digital aos chamados crimes de colarinho branco, que requerem determinado conhecimento técnico, entretanto, essa premissa tem se enfraquecido, visto

que, cada vez mais, pessoas sem sólidos conhecimentos em informática iniciam a prática delitiva e obtêm êxito.

Em exposição proferida em 2017, o ministro Alexandre de Moraes, integrante do Supremo Tribunal Federal, destacou que nem todos os crimes praticados no ambiente digital demandam a criação de novos tipos penais, pois, muitas vezes, a tecnologia funciona apenas como ferramenta para a prática de delitos já previstos no ordenamento jurídico tradicional (Jesus; Milagres, 2016). Um exemplo que ilustra essa perspectiva é a Lei n. 12.737/2012, que alterou o artigo 298 do Código Penal ao incluir os cartões de crédito e débito na definição de documento particular, reforçando sua proteção legal contra falsificações.

É importante observar que o "documento particular" constitui um elemento essencial da tipificação penal da conduta de falsificação. Na ausência desse elemento, a subsunção da conduta ao tipo penal se torna inviável. Nesse sentido, ao reconhecer explicitamente os cartões como documentos particulares, o legislador procurou assegurar maior efetividade à norma penal frente às novas modalidades de fraude (Jesus; Milagres, 2016).

Contudo, a redação adotada não solucionou integralmente os desafios interpretativos surgidos com o avanço tecnológico. A norma permaneceu omissa quanto à falsificação de documentos eletrônicos que não apresentam suporte físico, como arquivos armazenados em tokens ou pen drives. Diante disso, surge a dúvida: tais condutas seriam penalmente irrelevantes? Para evitar lacunas, seria mais adequado que o legislador ampliasse o conceito de documento particular, equiparando-o expressamente a dados, informações e declarações eletrônicas, independentemente de sua materialização física, abrangendo conteúdos de qualquer natureza (Jesus; Milagres, 2016).

É cediço que, pelo princípio da legalidade, não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal, conforme o artigo 1º do Código Penal. Ninguém pode ser responsabilizado por fato que a lei não considera penalmente relevante.

Necessário, portanto, que o Direito Penal brasileiro desenvolva meios e instrumentos eficazes para punir os crimes cibernéticos, acompanhando a evolução tecnológica e garantindo segurança à população.

Diante disso, possível extrair que a legislação brasileira sobre crimes cibernéticos ainda precisa evoluir significativamente. Persistem lacunas que precisam ser preenchidas, bem como a necessidade de atualização do Código Penal com dispositivos mais específicos ao meio virtual. Apenas com tais medidas será possível reduzir a incidência desses crimes, proteger a população e penalizar efetivamente os criminosos (Jesus; Milagres, 2016).

Existem os chamados crimes virtuais próprios, definidos como aqueles em que o sujeito ativo utiliza diretamente o sistema informático da vítima para a prática delituosa, fazendo do computador tanto o objeto quanto o meio do crime (Almeida; Mendonça;

Carmo, 2015). Esses crimes possuem natureza própria, pois dependem exclusivamente da existência do ambiente digital para ocorrer.

Para esclarecer o conceito de crime próprio, Cleber Masson (2019, p. 734) explica que:

> Crimes próprios ou especiais são aqueles em que o tipo penal exige uma situação de fato ou de direito diferenciada por parte do sujeito ativo. Apenas quem reúne as condições especiais previstas na lei pode praticá-lo. É o caso do peculato (CP, art. 312), cujo sujeito ativo deve ser funcionário público, e também do infanticídio (CP, art. 123), que precisa ser praticado pela mãe, durante o parto ou logo após, sob a influência do estado puerperal.

Mirabete e Fabbrini (2024, p. 440) prosseguem:

> Em se tratando de crimes próprios, o autor deve reunir os requisitos previstos no tipo para o sujeito ativo (ser funcionário público, médico etc.). Nada impede a coautoria ou a participação em delitos que tais, bastando que os colaboradores preencham os componentes subjetivos do tipo (o dolo e os demais elementos subjetivos do tipo).

Por outro lado, os crimes virtuais impróprios são aqueles cometidos com o auxílio de recursos tecnológicos, ou seja, por meio de um computador que funciona como instrumento para a realização de um ato ilícito que atinge um bem jurídico protegido previamente. Nesse sentido, Cunha (2021) destaca que esses crimes são tipificados no Código Penal tradicional, pois violam bens jurídicos comuns, especialmente a dignidade da pessoa humana, e utilizam meios informáticos apenas como ferramenta para a execução.

Em suma, resta claro que os crimes cibernéticos recebem diversas classificações na doutrina, podendo ser entendidos como exclusivos do ambiente digital, comuns, próprios ou impróprios, além de se manifestarem em formas instantâneas ou permanentes, simples ou complexas.

Apesar dessa variedade, todos compartilham um objetivo fundamental: causar danos e prejuízos que atingem a integridade física, moral, patrimonial ou psicológica das vítimas. O principal desafio para o sistema de justiça consiste na dificuldade de investigar e punir esses delitos, em virtude da natureza dinâmica, descentralizada e transnacional do meio virtual.

Conforme destaca Queiroz (2021), o Direito se apresenta como o único sistema normativo com autoridade legítima para conter o avanço da criminalidade digital, sendo também o único capaz de exercer coercitividade institucionalizada, por meio da tipificação, repressão e sanção de condutas consideradas ilícitas no ciberespaço.

Assim, compreendemos que os crimes cibernéticos são sim puníveis, havendo leis que permitem a responsabilização penal dos infratores. Todavia, tais normas ainda são insuficientes. Com o atual avanço tecnológico, torna-se evidente o descompasso entre as normas do Código Penal e a realidade contemporânea. Cabe, portanto, aos operadores do Direito a árdua missão de adequar os institutos penais às constantes inovações tecnológicas (Pacheco, 2011).

4 DIREITOS FUNDAMENTAIS E COLETIVOS PROTEGIDOS PELA CONSTITUIÇÃO FEDERAL

A característica mais relevante dos crimes cibernéticos é o meio pelo qual são praticados, ou seja, dependem essencialmente da tecnologia para sua concretização. Contudo, há delitos que não exigem, necessariamente, o uso da internet, como os crimes contra a honra. Ainda assim, é comum que tais infrações ocorram no ambiente virtual, impulsionadas pela sensação de impunidade, que, infelizmente, muitas vezes se confirma na prática.

Tais crimes geram impactos devastadores na sociedade, uma vez que não se limitam a atingir o patrimônio das vítimas, mas também causam danos de ordem psicológica e emocional, comprometem a reputação profissional, a privacidade, a imagem e até mesmo a liberdade sexual. Todos esses direitos são garantidos pela Constituição Federal, mas vêm sendo constantemente violados, com números alarmantes e em crescimento contínuo ao longo dos anos.

Além da esfera criminal, essas condutas também podem resultar em sanções civis. Um exemplo marcante foi a condenação do Facebook ao pagamento de R$ 10.000.000,00 (dez milhões de reais) por danos morais coletivos, além de R$ 500,00 (quinhentos reais) por dano moral individual a cada consumidor prejudicado pela liberação indevida de dados pessoais (Migalhas, 2024).

Entendido o conceito e as características desses crimes, resta saber: como ocorre, de fato, a invasão a dispositivos informáticos? A resposta é simples: é como se alguém invadisse sua casa, vasculhasse todos os cômodos, subtraísse seus pertences e saísse. Essa analogia representa um furto no mundo físico; contudo, quando a ação ocorre em meio virtual, é caracterizada como cibercrime. Ocorre que, por não estar tipificada de forma expressa e detalhada na legislação penal, tal conduta, até o presente momento, pode ser considerada atípica, o que evidencia a defasagem normativa frente à evolução tecnológica.

Um dos principais equívocos cometidos por parte da doutrina e do legislador é a confusão entre técnica e conduta. Para Damásio de Jesus e José Antônio Milagre (2016), o que importa juridicamente é a conduta realizada, independentemente da técnica utilizada.

Segundo os autores, o momento em que ocorre o ganho de acesso já configura o início dos atos executórios relacionados à invasão, enquanto as fases anteriores, como o perfilamento, a varredura e a enumeração, consistem em atos preparatórios, que ainda não são puníveis penalmente.

Os mesmos autores também defendem que, diante da realidade da sociedade da informação, não se pode admitir que prevaleçam práticas como a autotutela, a vingança privada ou a imposição da força. Para eles, é essencial que o Direito exerça sua função de garantir justiça e segurança nas relações entre os indivíduos no ambiente digital. Dessa forma, evidencia-se a urgente necessidade de o ordenamento jurídico acompanhar os avanços tecnológicos, assegurando à população mecanismos eficazes de proteção e responsabilização (Jesus; Milagres, 2016).

5 TRAMITAÇÃO DO PROJETO DE LEI DAS *FAKE NEWS* (PL 2630/2020)

O Projeto de Lei (PL) n. 2.630/2020, conhecido como "PL das *Fake News*", foi elaborado com o objetivo de combater a disseminação de informações falsas na internet. Essa iniciativa surgiu em resposta à crescente preocupação global com os impactos negativos da desinformação sobre a democracia e a convivência social (Cazaroti; Pinheiro, 2021).

No Brasil, a popularização da internet intensificou o desafio de conter boatos e notícias enganosas. Como essas informações se espalham rapidamente, tornou-se necessário pensar em formas eficazes de controle e em uma atualização legislativa que acompanhasse a realidade digital (Souza, 2021).

O referido projeto de lei baseia-se na premissa de que as *fake news* não se limitam a erros pontuais de informação, mas possuem o potencial de interferir em processos democráticos, manipular a opinião pública e até ameaçar vidas, como ocorreu durante a pandemia da Covid-19, período em que circularam diversos conteúdos falsos sobre tratamentos e formas de prevenção (Hernandez; De Toledo, 2021).

Antes da proposta do PL 2.630/2020, as legislações em vigor, como as Leis n. 12.735/2012 e 12.737/2012, tratavam de crimes cibernéticos de forma geral, mas não abordavam diretamente a propagação de desinformação (Dornelas, 2019).

Diversos acontecimentos revelaram os prejuízos concretos causados pelas *fake news*, como episódios de violência motivados por boatos e a influência em resultados eleitorais. Tais fatos evidenciaram a urgência da criação de normativas específicas para enfrentamento desse fenômeno (Krieguer; Ceron; Marcondes, 2021).

No entanto, o PL também tem gerado controvérsias. Alguns setores da sociedade manifestam preocupação com a possibilidade de a norma ser utilizada como instrumento

de censura ou de violação à privacidade dos usuários, levantando discussões sobre os desafios de equilibrar o combate à desinformação com a garantia dos direitos fundamentais (Calgaroto, 2021).

Diante de um cenário cada vez mais digitalizado e interconectado, especialistas defendem a atualização das legislações para lidar com os novos desafios tecnológicos. O PL das Fake news representa uma tentativa de o Brasil adequar seu ordenamento jurídico à realidade contemporânea (Martins Filho; Leite; Cerewuta, 2022).

Contudo, para que a aplicação da lei seja efetiva, é imprescindível que o Estado disponha de mecanismos adequados de investigação, capazes de enfrentar crimes digitais, incluindo a desinformação. A eficácia da norma, portanto, não depende apenas do conteúdo legislativo, mas também da capacidade de implementá-lo com eficiência (Silva; Silva, 2019).

O andamento do projeto reflete a preocupação crescente em adaptar o arcabouço jurídico às demandas oriundas do meio digital. Considerando o constante avanço da tecnologia, é provável que a legislação precise de revisões e aperfeiçoamentos contínuos (Lira; Salgado, 2021).

O PL busca, portanto, combater crimes cibernéticos associados à propagação de informações falsas, que, devido à facilidade de compartilhamento no meio virtual, podem acarretar impactos políticos, econômicos e sociais relevantes. Para tanto, propõe medidas regulatórias voltadas à prevenção dessas práticas.

Um dos dispositivos mais debatidos é a obrigatoriedade de que as plataformas digitais armazenem registros de mensagens enviadas em massa, com o intuito de rastrear os responsáveis por campanhas de desinformação. Contudo, essa medida levanta críticas quanto à possível violação da privacidade dos usuários, direito garantido pelo Marco Civil da Internet.

Outro ponto importante do projeto é a definição de contas falsas e *bots*, perfis automatizados utilizados para disseminar conteúdo em larga escala. A identificação desses agentes é essencial para coibir a manipulação de opinião pública.

A legislação enfrenta desafios devido à rapidez com que a tecnologia avança, contrastando com a morosidade do processo legislativo. Nesse sentido, o projeto também propõe maior transparência, exigindo que as plataformas informem os usuários sobre o alcance de conteúdos patrocinados, especialmente em contextos políticos e publicitários.

Ainda assim, a responsabilização penal dos autores de crimes digitais encontra dificuldades práticas, já que muitos agem anonimamente ou operam fora do território nacional. Existe um acordo internacional denominado Convenção de Budapeste, criado em 2001 pelos países da União Europeia, que estabelece diretrizes para o combate eficaz aos crimes cibernéticos, promovendo a harmonização das legislações entre os países signatários (Brasil, 2023. O Brasil, no entanto, ainda não integra essa convenção, o que

limita sua atuação no cenário internacional de cooperação jurídica e investigativa.

Por isso, é fundamental que as provas digitais sejam coletadas e preservadas de forma adequada, garantindo a efetividade dos processos judiciais.

Em síntese, o PL das *fake news* constitui uma resposta do legislador brasileiro aos desafios impostos pelos crimes digitais. Todavia, sua implementação deve considerar o equilíbrio entre a proteção da coletividade e a preservação de direitos fundamentais, como a liberdade de expressão e a privacidade. A aplicação da norma deve ser pautada por critérios técnicos e jurídicos que assegurem a justiça sem comprometer garantias individuais.

6 PLANO TÁTICO DE COMBATE A CRIMES CIBERNÉTICOS

Na realidade atual, a maior parte dos crimes virtuais ocorre não apenas em razão da sofisticação dos criminosos, mas, sobretudo, pela falta de conhecimento técnico dos usuários ao lidar com ferramentas digitais tão potentes quanto perigosas. Soma-se a isso o despreparo de parte das autoridades responsáveis pela investigação, além da banalização de golpes virtuais, muitas vezes encarados como algo distante, mas que, infelizmente, estão cada vez mais presentes no cotidiano e causam preocupação crescente.

Diante desse cenário, é fundamental refletir sobre a necessidade de uma legislação específica. Ainda que se reconheça que uma lei, por si só, não elimine completamente os crimes cibernéticos, ela é essencial para estabelecer parâmetros legais que possibilitem o julgamento adequado das condutas praticadas, contribuindo assim para a redução dos índices de delitos virtuais.

A evolução da informática e da tecnologia trouxe novas formas de se praticar antigos delitos. Crimes como ameaça, estelionato e extorsão continuam existindo, embora agora possam ser executados por meio digital. Essa transformação impõe desafios significativos ao Direito Penal, que precisa se adaptar a essa nova realidade sem perder sua efetividade.

Enquanto no Brasil ainda são tímidos os avanços em estrutura investigativa, países como Estados Unidos e Canadá têm convocado especialistas para integrar forças-tarefa voltadas exclusivamente ao combate de crimes cibernéticos. Nessas nações, o cibercrime já é classificado como uma das mais graves ameaças, superando inclusive o terrorismo. Por esse motivo, adotaram regulamentações rigorosas, desestimulando a atuação de *hackers* e outros agentes maliciosos no meio digital.

No panorama global, os crimes cibernéticos já ultrapassaram delitos como falsificação de documentos e tráfico de drogas, passando a ser encarados como uma questão de defesa nacional, além de segurança pública. Segundo pesquisa conduzida por Larry Ponemon (2019), renomado especialista em segurança e privacidade de dados, o Brasil figura como o segundo país com maior número de crimes cibernéticos, registrando um prejuízo de

aproximadamente 1 trilhão de dólares em apenas um ano.

Diante da pressão social e do aumento exponencial desses crimes, houve a criação da Lei n. 12.737/2012, conhecida como Lei Carolina Dieckmann (Brasil, 2012). À época, os criminosos conseguiram acessar e furtar arquivos pessoais, incluindo fotos íntimas, que posteriormente foram divulgadas na internet.

Além disso, ela foi alvo de tentativa de extorsão pelos invasores, que ameaçavam divulgar mais conteúdo caso suas exigências não fossem atendidas. Foram mais de 36 fotos íntimas divulgadas em redes sociais após não ceder à extorsão dos criminosos (Araújo, 2023). Embora tenha representado um avanço, a norma foi elaborada com foco nas técnicas utilizadas, o que se revelou um erro, considerando que os métodos cibernéticos evoluem constantemente.

O equívoco do legislador foi penalizar as técnicas ao invés de tipificar as condutas criminosas, o que torna a lei facilmente obsoleta diante do dinamismo das práticas digitais. Assim, o mais adequado seria atualizar o Código Penal, acrescentando a expressão "meio virtual" aos tipos penais já existentes, e reformular as normas punitivas com foco nas ações, e não nas ferramentas utilizadas.

Além da atualização legislativa, é fundamental que sejam adotadas medidas preventivas. Isso inclui o uso de senhas seguras, a atualização constante de softwares e a conscientização da população sobre os riscos virtuais. Contudo, a efetividade no combate aos cibercrimes também depende de um rigor legislativo maior e da cooperação internacional. Nesse sentido, Marcos Simplício, Ministro do Superior Tribunal de Justiça, destaca a necessidade de informar os cidadãos sobre práticas seguras na internet e de formar profissionais capacitados para fortalecer a segurança digital (Jesus; Milagres, 2016).

A solução mais viável para a contenção dos crimes virtuais está na atualização do Código Penal, na capacitação da polícia civil e de outros órgãos de segurança, e na adesão do Brasil à Convenção de Budapeste. Com essas medidas, será possível construir uma estrutura mais sólida de combate aos delitos cibernéticos, resultando em uma redução expressiva dessas ocorrências.

Esse plano estratégico deve incluir eixos temáticos voltados à prevenção e mitigação de ameaças cibernéticas; ao gerenciamento de riscos e incidentes; ao fortalecimento das infraestruturas críticas de proteção; ao aprimoramento do arcabouço jurídico e regulatório; à criação de parcerias nacionais e internacionais; à padronização e integração informacional; bem como ao fomento à pesquisa, à inovação e à educação digital voltadas ao enfrentamento da criminalidade cibernética.

Conforme apontam estudiosos como Jesus e Milagres (2016), é inadmissível permitir que, pela ausência de uma legislação eficaz, pessoas mal-intencionadas continuem utilizando computadores e redes sociais para fins ilícitos. Daí a urgência de uma norma específica que

defina os crimes informáticos e estabeleça suas respectivas penas, contribuindo para a segurança jurídica no ambiente digital.

7 CONSIDERAÇÕES FINAIS

Com este trabalho, foi possível compreender que, apesar das evoluções já promovidas no Código Penal, este ainda se mostra insuficiente para penalizar de forma eficaz os crimes cometidos por meio virtual. Nesse sentido, torna-se indispensável uma atualização legislativa mais profunda, com vistas à redução dos índices de criminalidade digital mencionados, bem como à conscientização da população e à capacitação dos agentes responsáveis pela investigação, a fim de promover maior segurança das informações no ambiente virtual.

Diante disso, é necessário destacar que os crimes cibernéticos ainda carecem de maior atenção do meio jurídico. Apesar da elevada quantidade de delitos cometidos diariamente no meio digital, os estudos voltados à prevenção e ao combate dessas práticas ainda são incipientes, revelando uma lacuna preocupante.

A internet, por sua natureza dinâmica e de alcance global, facilita a disseminação rápida de informações, incluindo notícias falsas (*fake news*), que podem ser veiculadas por qualquer usuário. Essa característica favorece a ação de estelionatários virtuais e indivíduos mal-intencionados que utilizam o anonimato proporcionado pela rede para ofender, difamar ou manipular suas vítimas, violando diversos princípios e direitos fundamentais previstos na Constituição Federal.

Conclui-se, portanto, que os crimes cibernéticos estão muito mais presentes no cotidiano digital do que se imagina. Muitos usuários sentem-se seguros para cometer delitos sob o manto do anonimato virtual, o que lhes confere uma falsa sensação de impunidade, encorajando condutas que, fora do ambiente digital, não ousariam praticar.

Ademais, observa-se uma constante evolução nos modus operandi utilizados pelos criminosos, com técnicas cada vez mais sofisticadas para ludibriar as vítimas e propagar desinformação. Dentre os crimes que mais preocupam, destaca-se o crescimento alarmante de práticas envolvendo pornografia infantil, muitas vezes hospedadas em camadas ocultas da internet, como a *deep web*, dificultando a identificação dos autores, usuários e a remoção do conteúdo ilícito.

No que se refere aos procedimentos investigativos, verifica-se que as provas digitais são essenciais para a responsabilização penal dos agentes. A efetiva condenação depende da comprovação inequívoca da autoria e da materialidade delitiva já na fase investigatória. Para isso, é indispensável a identificação e análise das evidências deixadas pelo criminoso, sendo fundamental o exame de corpo de delito digital, como o rastreamento do endereço IP utilizado, além da realização de perícias forenses por profissionais devidamente

qualificados.

Dessa forma, possível vislumbrar que as infrações cometidas em ambiente virtual encontram-se apenas parcialmente amparadas pelo ordenamento jurídico brasileiro, havendo ainda uma considerável lacuna quanto à tipificação penal de determinadas condutas.

Quanto aos métodos de investigação, torna-se fundamental o fortalecimento do aparato policial, o aperfeiçoamento técnico dos profissionais envolvidos na persecução penal e a ampliação da cooperação internacional. Tais medidas são imprescindíveis para a efetiva aplicação da legislação já existente e para a construção de um sistema de justiça criminal mais preparado para enfrentar os desafios impostos pela criminalidade digital.

Em suma, o presente estudo concluiu que a legislação penal brasileira, apesar das emendas pontuais (Lei 12.737/2012 e 14.155/2021), ainda carece de uma reforma estrutural capaz de enfrentar a alta sofisticação dos cibercrimes, levando à atipicidade de condutas e à insegurança jurídica.

Nesse sentido, e como principal proposição deste trabalho, reafirma-se a necessidade imperativa de o legislador brasileiro adotar uma abordagem sistêmica, com a adesão formal à Convenção de Budapeste e a modernização do Código Penal com foco na proteção do bem jurídico e na conduta, e não na mera ferramenta tecnológica utilizada.

REFERÊNCIAS

ALMEIDA, Jéssica de Jesus; MENDONÇA, Allana Barbosa; CARMO, Gilmar Passos do. **Crimes Cibernéticos.** 2015. 22 f. Trabalho de Conclusão de Curso (Graduação em Direito) – Universidade Tiradentes (UNIT), Estância, 2015.

ARAÚJO, Janaína. Dez anos de vigência da Lei Carolina Dieckmann: a primeira a punir crimes cibernéticos. **Senado Federal**, Brasília, DF: 2023. Disponível em: https://www12.senado.leg.br/radio/1/noticia/2023/03/29/dez-anos-de-vigencia-da-lei-carolina-dieckmann-a-primeira-a-punir-crimes-ciberneticos. Acesso em: 18 mai. 2025.

BRASIL. **Código Penal**. Decreto-Lei n. 2.848, de 7 de dezembro de 1940. Brasília, DF: Presidência da República, 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 24 out. 2024.

BRASIL. **Decreto n. 11.491, de 12 de Abril de 2023**. Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001. Brasília, DF: Presidência da República, 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/Decreto/D11491.htm. Acesso em:

10 mar. 2025.

BRASIL. **Lei n. 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos – Lei Carolina Dieckmann. Brasília, DF: Presidência da República, 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 24 out. 2024.

BRASIL. Superior Tribunal de Justiça (Quinta Turma). RHC 31.321/PR. Rel. Min. Marco Aurélio Bellizze, j:16/5/2013.

CALGAROTO, Cléber. **O Direito à Privacidade na Internet:** Panorama, Responsabilização Civil e Inovações do Marco Civil da Internet (Lei n. 12.965/2014). Trabalho de Conclusão de Curso (Graduação em Direito) - Unisul Virtual, 2021.

CARDOSO, Lucas de Holanda M. O Direito na Era Digital: O Cibercrime no Ordenamento Jurídico Brasileiro. **Cepein**, p. 1-12, 2017. Disponível em: https://cepein.femanet.com.br/BDigital/arqPics/1611400792P734.pdf. Acesso em: 10 fev. 2025.

CARVALHO, Ivan Lira de. O Direito Penal como Instrumento Inibidor da Violência. **Revista dos Tribunais**, *online*, v. 85, p. 463-470, 1996.

CAZAROTI, Tatiane Martins Barros; PINHEIRO, Eduardo Fernandes. **Crimes Cibernéticos.** Trabalho de Conclusão de Curso (Graduação em Direito) – Centro Universitário de Várzea Grande, Minas Gerais, 2021. Disponível em: https://repositoriodigital.univag.com.br/index.php/rep/article/view/203. Acesso em: 10 fev. 2025.

DORNELAS, Natália Alves. **A Resposta Estatal Quanto aos Crimes Cibernéticos:** Uma Análise Direcionada às Leis n. 12.735/2012 e 12.737/2012. Trabalho de Conclusão de Curso (Graduação em Direito) – Centro Universitário de Manhuaçu, Minas Gerais, 2019. Disponível em: https://www.pensaracademico.unifacig.edu.br/index.php/repositoriotcc/article/view/1727. Acesso em: 24 out. 2024.

HERNANDEZ, Erika Fernanda Tangerino; TOLEDO, Nathália Karina Abucci de. Crimes Cibernéticos: Seus Efeitos Revolucionários Diante de uma Legislação em Constante Evolução. **Revista Jurídica da UniFil**, Londrina, v. 17, n. 17, p. 72-84, 2021.

JESUS, Damásio de; MILAGRES, José Antônio. **Manual de Crimes Informáticos**. São Paulo: Saraiva, 2016.

KURTZ, João. **Registros de ocorrências de crimes virtuais aumentam 70% no país em 1 ano.** TechTudo, *online*, 2014. Disponível em: http://www techtudo.com.br/noticias/noticia/2014/10/registros-de-ocorrencias-de-crimes-virtuais-aumentam-770-no-pais-em-1 -ano.html. Acesso em: 10 fev. 2025.

KRIEGUER, André Lemuel Ferreira; CERON, Antonio Luciano Bairros; MARCONDES, Aldair. A Acelerada Evolução Social e Tecnológica Global como Viabilizadores de Crimes Cibernéticos, Frente ao Lento Desenvolvimento de Freios Legais para sua Contenção. **Ponto de Vista Jurídico**, *online*, p. 128-143, 2021.

LIRA, Caio César Dutra; SALGADO, Ana Alice Ramos Tejo. A Era Digital e a Prática de Crimes Cibernéticos: Uma Análise Sobre o Princípio da Extraterritorialidade. **Criminalidade na Era Digital**, *online*, v. 58046, p. 68, 2021.

MARANHÃO, David Vinicius do Nascimento. As Novas Disposições sobre os Crimes Cibernéticos. **JusBrasil**, *online*, 2022. Disponível em: https://davidsviniciusadv.jus.com.br/publicacoes. Acesso em: 23 nov. 2024.

MARTINS FILHO, Rogério; LEITE, Roniel Bispo; CEREWUTA, Pollyanna Marinho Medeiros. A Ascensão dos Crimes Cibernéticos no Contexto Contemporâneo. **Facit Business and Technology Journal**, *online*, v. 1, n. 37, 2022.

MASSON, Cleber. **Direito Penal:** Parte Geral. 13. ed. Rio de Janeiro: Forense, 2019.

MIGALHAS. Facebook é condenado a pagar R$ 500 a cada usuário por falha técnica. **Migalhas.com**, *online*, 2024. Disponível em: https://www.migalhas.com.br/quentes/410863/facebook-e-condenado-a-pagar-r-500-a-cada-usuario-por-falha-tecnica. Acesso em: 19 nov. 2024.

MIRABETE, Julio Fabbrini; FABBRINI, Renato N. **Manual de Direito Penal**. 36. ed. Indaiatuba, SP: Editora Foco, 2024.

PACHECO, Wilfredo Enrique Pires. Manual de Responsabilização Penal dos *Hackers*, Crackers, e Engenheiros Sociais. **Consultor Jurídico**, São Paulo, v. 2011, p. 1, 2011.

NEOTEL. Tentativas de Ciberataques crescem 21% no segundo semestre de 2022 **Neotel**, *online*, 2023. Disponível em: https://blog.neotel.com.br/sem-categoria/tentativas-de-ciberataques-crescem-21-no-segundo-semestre-de-2022/. Acesso em: 10 abr. 2025.

PINHEIRO, Patrícia Peck. Regulamentação da Web. **Cadernos Adenauer**, Rio de Janeiro, v. 15, n. 4, p. 33-44, out. 2014. Disponível em: http://www.kas.de/wf/doc/16471-1442-5-

30.pdf. Acesso em: 2 out. 2024.

PONEMON, Larry. Cyberattacks on SMBs Rising Globally, Becoming More Targeted and Sophisticated. **Ponemon Sullivan Provacy Report**, *online*,2019. Disponível em: https://ponemonsullivanreport.com/2019/12/. Acesso em: 10 fev. 2025.

QUEIROZ, Gabriel Ferreira. **Cibercriminalidade no Brasil:** Aplicação, Falibilidade e Impunidade. Trabalho de Conclusão de Curso (Graduação em Direito) – Escola de Direito e Relações Internacionais, Curso de Direito, da Pontifícia Universidade Católica de Goiás (PUCGOIÁS), 2021. Disponível em: https://repositorio.pucgoias.edu.br/jspui/bitstream/123456789/2960/1/TCC-%20GABRIEL%20FERREIRA%20QUEIROZ%20%20.pdf. Acesso em: 10 fev. 2025.

SCHJOLBERS, Stein. The History of Global Harmonization on Cibercrime Legislation: The Road to Geneva. **CyberCrime Law**, *online*, 2008.

SILVA, Kaique Rodrigues; SILVA, Rubens Alves da. Crimes Cibernéticos: Necessidade de Novas Ferramentas de Investigação com Encargos no Ônus da Prova. **Revista Artigos.com**, *online*, v. 12, p. e2480-e2480, 2019.

SOUZA, Alexandre Dourado Gomes de. **O Avanço dos Crimes Cibernéticos:** Um Estudo Sobre os Crimes Previstos nas Leis 12.737/2012 e 12.735/2012 e a Importância da Materialidade da Prova e seus Reflexos no Ataque Cibernético na Rede de Informática do Superior Tribunal de Justiça em 2020. 18f. Trabalho de Conclusão de Curso (Graduação em Direito) - Centro Universitário dos Guararapes (UNIFG), Guararapes, 2021.

Declaração de uso de Inteligência Artificial

Este artigo contou com o uso de ferramenta de Inteligência Artificial (IA), especificamente o ChatGPT 4.0, empregada unicamente para fins de tradução. O uso da IA respeita integralmente as normas editoriais da Revista Jurídica UNIGRAN, conforme declarado no Termo de Autorização de Publicação. A autora assume total responsabilidade pela originalidade, precisão e integridade do conteúdo apresentado.