172. O DIREITO NA ERA DIGITAL: COMBATE E PREVENÇÃO DE CRIMES CIBERNÉTICOS

Mayume Caires Moreira
Mestra, Unicesumar.
Maringá – Paraná – Brasil
http://lattes.cnpq.br/0329252013346411
https://orcid.org/0000-0001-8163-7406
Mayume.moreira@unicesumar.edu.br

Camila Goes Hervatini
Graduanda, Unicesumar.
Maringá – Paraná - Brasil
ra-24218415-2@alunos.unicesumar.edu.br
https://lattes.cnpq.br/7986768751281016

Tainá Theodoro Scola
Graduanda, Unicesumar.
Maringá – Paraná – Brasil
http://lattes.cnpq.br/0652515190050898
ra-24011128-2@alunos.unicesumar.edu.br

RESUMO

O avanço das tecnologias digitais tem transformado significativamente a sociedade contemporânea, trazendo inúmeros benefícios nas áreas da comunicação, do acesso à informação, das relações comerciais e da gestão pública. No entanto, esse progresso também tem aberto espaço para o surgimento e a intensificação dos crimes cibernéticos, os quais representam uma crescente ameaça à segurança, à privacidade e aos direitos fundamentais dos indivíduos. Neste contexto, o estudo tem como tema o enfrentamento jurídico dos crimes cibernéticos e a sua prevenção, cuja relevância se justifica pela urgência de se refletir sobre os mecanismos jurídicos disponíveis para enfrentar tais condutas, considerando a crescente dependência digital da sociedade e os desafios impostos à legislação atual. O problema de pesquisa que se impõe em quais são os principais desafios enfrentados pelo direito brasileiro na prevenção e repressão aos crimes cibernéticos, e quais estratégias podem ser adotadas para sua superação? O presente artigo tem como objetivo analisar de forma crítica as estratégias de combate e prevenção do direito frente aos crimes digitais, destacando as dificuldades e as possibilidades de atuação do sistema jurídico. Para isso, foi realizada uma revisão bibliográfica ampla sobre os cibercrimes e as legislações que abordam o assunto, utilizando o método dedutivo, com enfoque na legislação brasileira, nos principais tipos de crimes cibernéticos, como fraudes eletrônicas, roubo de dados e invasões de dispositivos, bem como nas formas de prevenção. Conclui-se que, para o combate eficaz aos crimes cibernéticos, é fundamental uma abordagem mais integrada, que envolva a constante atualização da legislação, o fortalecimento das instituições de segurança e justiça, bem como uma mudança cultural que promova a conscientização sobre o uso ético e seguro das tecnologias digitais.

PALAVRAS-CHAVE: Desinformação. Privacidade Online. Proteção de Dados.

ABSTRACT

The advancement of digital technologies has significantly transformed contemporary society, bringing numerous benefits in the areas of communication, access to information, commercial relations, and public administration. However, this progress has also created space for the emergence and intensification of cybercrimes, which pose a growing threat to the security, privacy, and fundamental rights of individuals.

In this context, the study focuses on the legal confrontation and prevention of cybercrimes, whose relevance lies in the urgent need to reflect on the legal mechanisms available to address such conduct, considering society's increasing digital dependence and the challenges imposed on current legislation.

The guiding research question is: What are the main challenges faced by Brazilian law in preventing and repressing cybercrimes, and what strategies can be adopted to overcome them?

This article aims to critically analyze the strategies used by the legal system to combat and prevent digital crimes, highlighting the difficulties and possibilities for legal action. To this end, an extensive bibliographic review was conducted on cybercrimes and the legislation addressing the issue, employing the deductive method, with emphasis on Brazilian law, the main types of cybercrimes—such as electronic fraud, data theft, and device intrusion—as well as prevention measures.

The study concludes that, for an effective fight against cybercrimes, a more integrated approach is essential, involving the constant updating of legislation, the strengthening of security and justice institutions, and a cultural shift that promotes awareness regarding the ethical and safe use of digital technologies.

Keywords: Disinformation; Online Privacy; Data Protection.

1 INTRODUÇÃO

O presente estudo tematiza a análise dos crimes cibernéticos e a prevenção e combate do direito. O tema em questão desempenha um papel crucial e fundamental que está diretamente ligado à segurança, privacidade e à proteção dos direitos fundamentais no ambiente digital. Assim, com o aumento da digitalização no cotidiano por meio de serviços bancários, saúde e trabalho remoto, a exposição desses indivíduos a uma série de vulnerabilidades no ambiente virtual tem se tornado frequente. O mundo contemporâneo vive uma revolução digital sem precedentes, e com ela surgem novos desafios jurídicos e sociais que exigem respostas rápidas e eficazes do poder público e da sociedade.

Nesse contexto, os crimes cibernéticos têm se multiplicado de forma alarmante, acompanhando a expansão do uso da internet e das novas tecnologias de informação e comunicação. A variedade e complexidade dessas condutas criminosas que incluem desde fraudes eletrônicas e clonagem de cartões até invasões de dispositivos, roubo de dados, disseminação de fake news, discursos de ódio e assédio virtual tornam o combate a essas práticas um campo de grande complexidade para o direito. Além disso, a natureza transnacional da internet dificulta a delimitação de jurisdições e a efetivação das normas legais, criando obstáculos à responsabilização dos autores dessas infrações.

Dessa maneira, o estudo se torna relevante, uma vez que os crimes digitais ameaçam valores fundamentais garantidos pela Constituição Federal, como o direito à intimidade, à honra, à imagem e à liberdade de expressão, ao mesmo tempo em que revelam lacunas legislativas e estruturais no enfrentamento dessas práticas. A celeridade com que novas modalidades de cibercrimes surgem torna evidente a necessidade de que o ordenamento jurídico acompanhe as transformações tecnológicas. Outrossim, a atuação eficiente do Estado no combate a esses delitos depende da integração entre o aparato jurídico, as forças de segurança, os operadores do direito e as próprias plataformas digitais.

O intuito desse projeto é demonstrar para a sociedade como compreender a dinâmica dos crimes cibernéticos é crucial não apenas para a eficácia do sistema jurídico, mas também para a segurança pública e o bem-estar da sociedade como um todo. Ademais, a intensa sofisticação das organizações criminosas no mundo virtual destaca a

necessidade de uma resposta legal mais eficaz, estruturada e tecnológica. A legislação vigente, embora contenha avanços significativos como a promulgação do Marco Civil da Internet (Lei nº 12.965/214) e a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), ainda carece de atualização constante e de mecanismos operacionais para aplicação prática efetiva.

Diante desse cenário, o problema de pesquisa que norteia este estudo pode ser formulado da seguinte forma: quais são os principais desafios enfrentados pelo direito brasileiro na prevenção e repressão aos crimes cibernéticos, e quais estratégias podem ser adotadas para sua superação? O objetivo geral do trabalho consiste em analisar criticamente os instrumentos jurídicos disponíveis no Brasil para o enfrentamento dos crimes digitais, identificando suas limitações, possibilidades de aprimoramento e o papel da educação digital como ferramenta preventiva.

Portanto, enquanto a internet se torna a principal fonte de acesso a informações para buscar novos conhecimentos, ela se transforma em uma ferramenta perigosa para a propagação de acusações falsas, violências, inverdades com mínima ou nenhuma possibilidade de penalização aos infratores. Este estudo ao abordar tais questões, pretende contribuir para o debate acadêmico e social sobre a necessidade de um direito robusto, eficaz e adaptado às novas realidades tecnológicas.

2 REFERENCIAL TEÓRICO

Crimes cibernéticos, também chamados de crimes virtuais, cibercrimes crimes digitais, entre outras nomenclaturas. São dados as condutas ilícitas em que se utiliza um computador ou rede para cometer delitos. Tendo em seu alvo dados pessoais, financeiros, sistemas computacionais ou até pessoas jurídicas e físicas. De acordo com a Convenção de Budapeste (2004) sobre os crimes cibernéticos, que é um acordo internacional que visa combater os cibercrimes por meio da cooperação entre os países signatários, os crimes virtuais englobam infrações como acesso não permitido, intercepção de dados, interferência em sistemas e a utilização imprópria de aparelhos tecnológicos para fins ilícitos.

Os crimes virtuais são divididos em dois tipos: crimes próprios e impróprios. Os próprios só existem no mundo digital, exemplo: invasão de dispositivo e disseminação de vírus. Já os impróprios usam a internet para cometer crimes que também podem acontecer fora dela, exemplo: estelionato e fraude em internet banking. A variedade e complexidade

desses delitos demandam uma tática jurídica abrangente, que inclua tanto o aspecto penal quanto o civil, administrativo e internacional.

A legislação cibernética no Brasil mudou muito nos últimos anos, sendo motivada pela necessidade de acompanhar o progresso tecnológico e combater as novas formas de criminalidade digital. Inicialmente, a legislação brasileira não possuía regras específicas para o ambiente digital, o que criava brechas na tipificação penal e dificultava a punição dos autores de crimes praticados por meio da internet. Com a expansão acelerada do uso das redes digitais, tornou-se essencial o desenvolvimento de ferramentas jurídicas apropriadas à realidade do ambiente digital. Para DONEDA (2019, p.124), ‘’a legislação penal brasileira ainda não consegue acompanhar com precisão a velocidade com que surgem novos comportamentos lesivos no meio digital’’, o que compromete a efetividade da responsabilização jurídica. O autor destaca que, embora existam avanços, a tipificação penal ainda enfrenta desafios para lidar com as particularidades do ciberespaço, o que exige constantes ajustes nas normas legais.

A Lei "Carolina Dieckmann" nº 12.737/2012 foi um marco no combate à criminalidade digital no Brasil. Esta legislação foi estabelecida após o vazamento de imagens íntimas da atriz que lhe dá nome, e passou a classificar ações como a invasão de aparelhos eletrônicos com o propósito de obter, alterar ou apagar informações sem o consentimento do proprietário (Brasil,2012).

Promulgada em 2014, a Lei 12.965 é conhecida como Marco Civil da Internet, que define direitos, deveres, princípios e garantias para a utilização da internet no Brasil. O Marco Civil estabelece normas para a proteção da privacidade dos usuários, a neutralidade da rede, responsabilidade dos provedores de serviços e a liberdade de expressão. Reconhecida como uma legislação pioneira e referência mundial (Brasil,2014).

Instituída em 2018 pela Lei nº 13.709, a Lei Geral de Proteção de Dados Pessoais (LGPD) busca proteger a privacidade e a integridade dos dados pessoais no ambiente digital. Ela define diretrizes claras para a gestão de dados privados por empresas, entidades governamentais e privadas, além de aplicar penalidades para vazamentos ou usos impróprios desses dados. Essas normas, apesar de relevantes, evidenciam a necessidade contínua de atualização e adequação das normas para acompanhar o crescimento da complexidade dos crimes cibernéticos e assegurar a eficácia da resposta jurídica (Brasil,2018).

O combate aos crimes cibernéticos no Brasil apresenta uma série de entraves estruturais, legais e operacionais. A natureza dinâmica e transnacional dessas infrações dificulta a atuação das autoridades policiais e judiciais, exigindo soluções complexas e integradas. Um dos principais desafios está relacionado à dificuldade de identificação e responsabilização dos infratores, que frequentemente operam com o uso de mecanismos de anonimização, como redes privadas virtuais (VPNs), criptografia de ponta a ponta e navegação em camadas (deep web). Tais recursos tecnológicos tornam o rastreamento mais complexo, exigindo ferramentas forenses especializadas e atuação técnica de alto nível. Nesse sentido, BLUM (2013, p.85) destaca que ‘’as barreiras geográficas deixam de ser obstáculos e passam a ser instrumentos usados pelos criminosos para impedir sua responsabilização’’, evidenciando como o ambiente digital favorece a impunidade diante das limitações jurisdicionais e técnicas enfrentadas pelos sistemas de segurança e justiça.

Outro desafio relevante é a defasagem tecnológica e estrutural dos órgãos de segurança pública, que frequentemente não dispõem dos recursos materiais e humanos necessários para uma atuação efetiva. A escassez de delegacias especializadas, especialmente em estados do interior e regiões mais afastadas dos grandes centros urbanos, compromete a uniformidade e a celeridade no enfrentamento desses delitos. Além disso, há uma carência de capacitação contínua de profissionais da segurança pública, do Ministério Público e do Judiciário em relação às particularidades técnicas dos crimes digitais.

A ausência de normatização adequada para determinados tipos de condutas também é um problema. Embora o ordenamento jurídico brasileiro tenha avançado com a Lei Carolina Dieckmann (Lei nº 12.737/2012), o Marco Civil da Internet (Lei nº 12.965/2014) e a Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018), ainda existem lacunas em relação a práticas criminosas emergentes, como o uso indevido de inteligência artificial para manipulação de vídeos (deepfakes), fraudes com criptomoedas e crimes cibernéticos associados ao metaverso e outras realidades virtuais.

Por fim, a cooperação internacional limitada dificulta a responsabilização de criminosos que operam a partir de outros países. Muitos servidores utilizados para a prática de crimes estão localizados no exterior, e a ausência de tratados específicos ou a morosidade dos trâmites internacionais pode inviabilizar investigações ou retardar a produção de provas digitais, prejudicando a efetividade da persecução penal.

Diante dos desafios apresentados, é essencial adotar estratégias amplas de enfrentamento, com foco na repressão, prevenção e conscientização. Luiz Flávio Gomes destaca que o direito penal tradicional é insuficiente, exigindo atualização legislativa e práticas investigativas eficazes. A prevenção começa pela educação digital, com a inclusão de temas como segurança da informação e cidadania digital nas escolas. formando cidadãos mais conscientes e preparados para lidar com os riscos virtuais.

Campanhas públicas de conscientização também são ferramentas importantes. O poder público pode, por meio de parcerias com o setor privado e organizações da sociedade civil, desenvolver iniciativas que alertem a população sobre os perigos mais comuns, como golpes de phishing, engenharia social e roubo de identidade digital. O conhecimento é uma das formas mais eficazes de empoderar o usuário e reduzir a incidência de crimes.

No âmbito institucional, destaca-se a importância do fortalecimento das delegacias especializadas em crimes cibernéticos, com investimentos em equipamentos, softwares e capacitação técnica. A criação de núcleos interinstitucionais que integrem polícias civis, Ministérios Públicos, peritos forenses e agências de inteligência pode proporcionar respostas mais rápidas e coordenadas a incidentes cibernéticos de maior gravidade.

A cooperação internacional, por sua vez, deve ser aprimorada por meio da adesão a tratados multilaterais e à participação ativa em fóruns globais de cibersegurança. A Convenção de Budapeste, por exemplo, representa um marco importante na harmonização da legislação e na cooperação entre os países no combate aos crimes cibernéticos. O Brasil, embora ainda não seja signatário, vem estudando sua adesão, o que pode representar um avanço significativo nesse cenário.

O setor privado também tem papel central nesse processo. Empresas de tecnologia, provedores de serviços de internet e plataformas digitais devem atuar de forma responsável e colaborativa, oferecendo canais seguros de denúncia, preservando dados para investigação e investindo em medidas de proteção como autenticação de dois fatores, criptografia e inteligência artificial para detecção de comportamentos suspeitos.

3 METODOLOGIA

Este estudo empregou o método dedutivo, estabelecendo premissas gerais sobre o papel do direito na sociedade virtual como ponto de partida para uma análise lógica e estruturada das estratégias de combate e prevenção aos delitos cibernéticos. A investigação foi conduzida por meio de uma revisão bibliográfica abrangente, alicerçada em

artigos científicos que exploram o direito digital e a criminalidade online. Esse processo sistemático permitiu identificar os principais desafios enfrentados pelos profissionais do direito ao lidar com as novas modalidades de crimes perpetrados no ambiente virtual, bem como as estratégias promissoras para sua prevenção eficaz.

A opção pela revisão bibliográfica como metodologia de investigação se justifica intrinsecamente pela natureza teórica do problema em questão, ressaltando a necessidade crucial de compilar e analisar criticamente a vasta produção acadêmica existente sobre o tema. Foram criteriosamente selecionadas obras de relevância publicadas em periódicos científicos renomados, livros especializados e documentos legais acessíveis em bases de dados confiáveis, tais como Google Acadêmico e o Portal de Periódicos da CAPES. A análise aprofundada do conteúdo dessas fontes primárias possibilitou uma compreensão detalhada da evolução do arcabouço jurídico direcionado ao ambiente digital, com ênfase especial nas condutas criminosas praticadas no ciberespaço e nas dificuldades inerentes à aplicação das normas vigentes pelos operadores do direito.

O recorte temporal da pesquisa priorizou consistentemente publicações dos últimos dez anos, visando assegurar a atualidade das discussões e incorporar o impacto significativo das inovações tecnológicas recentes, como a crescente utilização da inteligência artificial, a onipresença das redes sociais e a emergência das criptomoedas no intrincado contexto dos crimes cibernéticos. Adicionalmente, foram considerados documentos normativos de importância fundamental, a exemplo da Lei nº 12.965/2014 (o Marco Civil da Internet), da Lei nº 13.709/2018 (a Lei Geral de Proteção de Dados Pessoais – LGPD) e de dispositivos pertinentes do Código Penal Brasileiro aplicáveis à temática em análise. Essas referências legais sólidas forneceram a base normativa essencial para a análise crítica dos mecanismos de responsabilização e prevenção existentes, oferecendo um panorama mais completo do cenário jurídico atual.

Outrossim, o estudo buscou abordar o tema de maneira intrinsecamente interdisciplinar, estabelecendo conexões significativas entre conceitos do direito penal, da segurança da informação e da ética digital. Essa abordagem holística permitiu uma compreensão mais abrangente e multifacetada dos impactos sociais e jurídicos da criminalidade online, contribuindo de forma substancial para a elaboração de propostas inovadoras que favoreçam tanto a repressão eficaz quanto a prevenção proativa desses delitos complexos.

Em suma, a metodologia rigorosa adotada neste estudo caracterizada pela sua clareza, sistematicidade e sólida fundamentação teórica almeja garantir a validade intrínseca dos resultados obtidos e, simultaneamente, possibilitar sua replicação por outros pesquisadores interessados, fortalecendo assim o debate acadêmico essencial sobre o papel crucial do direito na contemporânea era digital e os desafios prementes da justiça diante da crescente complexidade e sofisticação dos crimes cibernéticos. Acreditamos que esta abordagem metodológica robusta fornecerá insights valiosos para a área do direito digital.

RESULTADOS ALCANÇADOS

Apesar dos avanços legislativos e institucionais, o Brasil ainda enfrenta sérios desafios no combate aos crimes cibernéticos. A falta de investimentos em infraestrutura digital de investigação, a ausência de capacitação sistemática dos operadores do direito e a morosidade na cooperação internacional revelam uma lacuna preocupante entre o crescimento da criminalidade digital e a capacidade estatal de enfrentá-la.

O papel do direito, portanto, deve ser não apenas o de punir, mas também o de proteger, orientar e prevenir. Para isso, é necessário um esforço conjunto entre o poder público, o setor privado e os cidadãos, com vistas à construção de um ambiente digital mais ético, seguro e justo para todos.

Nesse contexto, é urgente que o Estado brasileiro adote uma postura proativa, com políticas públicas voltadas à digitalização da segurança, à formação interdisciplinar e à ampliação de canais de denúncia acessíveis à população. Além disso, o setor privado deve assumir a responsabilidade no combate à criminalidade digital, especialmente as empresas de tecnologia que dominam o ambiente virtual.

A formação de uma sociedade digital consciente passa pela inclusão da educação digital nas escolas, o incentivo à literacia tecnológica e o fortalecimento da cultura da privacidade e da proteção de dados. Tais ações, quando aliadas a um sistema jurídico adaptado e eficiente, podem reduzir significativamente a incidência de práticas criminosas no meio virtual. Garantir um ciberespaço mais seguro não é apenas uma missão institucional, é um compromisso coletivo com a liberdade, a

dignidade e a proteção da vida digital.

A análise realizada durante o desenvolvimento deste estudo permitiu constatar que o combate efetivo aos crimes cibernéticos depende de uma resposta jurídica mais dinâmica

e atualizada. Observou-se que as leis atualmente em vigor, embora representem avanços significativos, ainda não são plenamente eficazes diante da complexidade e da velocidade com que os crimes digitais evoluem. A morosidade nos processos judiciais, a dificuldade de rastreamento dos criminosos e a limitação de recursos tecnológicos disponíveis às autoridades competentes são alguns dos principais entraves identificados.

Outro resultado importante foi a constatação de que a maioria da população ainda não possui conhecimento adequado sobre seus direitos digitais, nem sobre os meios disponíveis para denunciar e se proteger contra crimes virtuais. Isso reforça a necessidade de políticas públicas voltadas à educação digital, desde o ensino básico até a formação profissional continuada. A conscientização sobre os riscos do ambiente virtual e o uso seguro das tecnologias são pilares fundamentais para a prevenção.

Ademais, concluiu-se que a cooperação internacional é indispensável no enfrentamento dessa modalidade criminosa, dado seu caráter transnacional. Parcerias entre países, bem como protocolos de compartilhamento de informações entre empresas de tecnologia e órgãos públicos, podem acelerar investigações e reduzir a impunidade. Assim, os resultados obtidos demonstram que o combate aos crimes cibernéticos exige uma abordagem ampla e integrada, capaz de aliar tecnologia, legislação e educação para garantir a segurança e a proteção dos direitos fundamentais no espaço digital.

REFERÊNCIAS

BLUM, Renato Opice. Direito digital: internet e os tribunais. 5. ed. São Paulo: Revista dos Tribunais, 2013.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 18 abr. 2025.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 18 abr. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 18 abr. 2025.

BRASIL. Ministério da Justiça e Segurança Pública. Crimes Digitais. Disponível em: https://www.gov.br/mj/pt-br/assuntos/sua-protecao/sedigi/crimes-digitais. Acesso em: 16 abr. 2025.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de Proteção de Dados. São Paulo: Thomson Reuters Brasil, 2019.

GOMES, Luiz Flávio. Crimes cibernéticos: comentários à Lei nº 12.737/2012 (Lei Carolina Dieckmann). São Paulo: Revista dos Tribunais, 2011.

MAIA, Teymisso Sebastian Fernandes. Análise dos mecanismos de combate aos crimes cibernéticos no sistema penal brasileiro. 2017. 114 f. Monografia (Graduação em Direito) – Faculdade de Direito, Universidade Federal do Ceará, Fortaleza, 2017. Disponível em: https://repositorio.ufc.br/handle/riufc/31996. Acesso em: 18 abr. 2025.

NIC.br. Classificação dos crimes cibernéticos. Disponível em: https://www.nic.br/noticia/na-midia/classificacao-dos-crimes-ciberneticos/. Acesso em: 16 abr. 2025.

SANTOS, João. A evolução dos crimes cibernéticos e os desafios da legislação brasileira. Revista FT, [S. l.], 2023. Disponível em: https://revistaft.com.br/a-evolucao-dos-crimes-ciberneticos-e-os-desafios-da-legislacao-brasileira/. Acesso em: 20 abr.2025