

153. CRIMES CIBERNÉTICOS: CONCEITO E DESAFIOS ENFRENTADOS PELO BRASIL

Camila Virissimo Rodrigues da Silva Moreira

Mestra em Ciências Jurídicas, UniCesumar.

Maringá – Paraná – Brasil

<https://orcid.org/0009-0000-3911-9699>

<https://lattes.cnpq.br/8591500782530359>

camila.moreira@docentes.unicesumar.edu.br

Henrique Tissei Jacomini

Graduando, Unicesumar.

Maringá – Paraná – Brasil

<https://orcid.org/0009-0006-2334-2021>

ra-24066424-2@alunos.unicesumar.com

Vitor Caires Soldá Bressanin

Graduando, Unicesumar.

Maringá – Paraná – Brasil

<https://orcid.org/0009-0000-8984-8267>

ra-24131981-2@alunos.unicesumar.edu.br

Walter Neto Borges Santana

Graduando, Unicesumar.

Maringá – Paraná – Brasil

<https://orcid.org/0009-0001-2823-9967>

ra-24066417-2@alunos.unicesumar.com

RESUMO

Este trabalho científico explora a crescente prevalência dos crimes cibernéticos no Brasil, frequentemente observável no ambiente virtual, este que deveria facilitar inúmeras atividades cotidianas, serve como um terreno fértil para a prática de delitos como furto, estelionato, difamação, extorsão e outros crimes que são cada vez mais comuns, devido à sensação de impunidade percebida pelos infratores que atuam na penumbra do anonimato favorecida pelo uso da internet e aparelhos eletrônicos. O objetivo deste trabalho é conceituar os crimes cibernéticos e compreender os desafios enfrentados pelo sistema jurídico brasileiro no combate a essas práticas delituosas. Utilizou-se neste trabalho o método de pesquisa hipotético dedutivo, o qual envolve a revisão da legislação brasileira, de bibliografia, documentos, e textos jurídicos especializados para analisar a tipificação dos crimes cibernéticos e a evolução do ordenamento jurídico brasileiro no combate a esses delitos, a fim de entender o contexto histórico, normativo e institucional. Foi obtido a partir deste estudo a elucidação doutrinária sobre os cibercrimes e quem os cometem, assim como seus motivos, e a compreensão das estratégias que podem ser adotadas para amenização deste problema, que não ocorre pela inexistência de normas e sim pela não incidência da legislação. Conclui-se a partir deste trabalho, que a evolução tecnológica não trouxe somente benefícios, existindo os malefícios dos crimes cibernéticos, portanto, visando amenizar o problema, é necessário a transparência das normas, além de políticas públicas voltadas à capacitação de profissionais, educação digital e ao investimento em tecnologias de segurança cibernética.

PALAVRAS-CHAVE: Cibercrime; Virtual; Legislação.

ABSTRACT

This scientific study explores the growing prevalence of cybercrimes in Brazil. Often observed in the virtual environment—which should facilitate numerous daily activities—this space has instead become fertile ground for offenses such as theft, fraud, defamation, extortion, and other increasingly common crimes. This rise is partly due to the sense of impunity perceived by offenders operating under the anonymity facilitated by the use of the internet and electronic devices. The objective of this study is to define cybercrimes and understand the challenges faced by the Brazilian legal system in combating these unlawful practices. The research employed the hypothetical-deductive method, involving a review of Brazilian legislation, bibliographic sources, documents, and specialized legal texts to analyze the classification of cybercrimes and the evolution of the Brazilian legal framework in addressing these offenses, aiming to understand the historical, normative, and institutional context. This study provided doctrinal clarification on cybercrimes, the profiles of those who commit them, their motives, and the strategies that can be adopted to mitigate the problem—which persists not due to

a lack of laws, but due to their insufficient enforcement. It is concluded that technological advancement has not brought only benefits, as cybercrime poses significant harms. Therefore, to mitigate this issue, transparency in regulations is essential, along with public policies focused on professional training, digital education, and investment in cybersecurity technologies.

Keywords: Cybercrime; Virtual; Legislation.

1 INTRODUÇÃO

Cotidianamente várias pessoas utilizam dos meios eletrônicos, não restando dúvidas de que este é o momento de toda a história da humanidade, em que as vidas das pessoas estão amplamente conectadas, seja para buscar informações, conversar nas redes sociais, por videoconferência ou chamadas, trabalhar, executar operações bancárias, e-mails. Em pesquisa realizada pelo Instituto Nacional de Combate ao Cibercrime (INCC, 2024, p. 14), foi constatado que no Brasil, segundo levantamento feito pela FGV no ano de 2023, existem 464 milhões de dispositivos digitais (computador, notebook, smartphone e tablet) ativos, considerando o uso doméstico e corporativo, confirmando a ampla utilização da tecnologia no país.

Deste modo, ao passo que a tecnologia evolui e se prolifera entre a sociedade, o mundo virtual se torna um ambiente cada vez mais habitado. Surge então neste novo meio, a prática de delitos caracterizados como crimes cibernéticos, e estes possuem uma capacidade de evolução que desafia não só o nosso país, mas também o resto do mundo. Sendo assim, é necessário a conceituação do que são os crimes cibernéticos, dada a complexidade do tema, por se tratar de um cenário que teve várias mutações nas últimas décadas, possuindo múltiplas faces.

É necessário também compreender a autoria desses delitos, ou seja, a motivação dos criminosos para a execução de tal ato, para que medidas eficazes possam combater esse fenômeno. Em uma breve contextualização, os crimes cibernéticos surgiram já no início da computação, quando esses atos ilícitos eram executados apenas pela curiosidade e desafio técnico. Entretanto, com a rápida evolução e expansão da tecnologia, aumentaram também as motivações dos criminosos, como o ciberterrorismo, espionagem, vandalismo, revanchismo, enriquecimento ilícito e outras formas que afetam a segurança pública.

Nesse sentido, ao se observar a legislação brasileira no que diz respeito aos crimes cibernéticos, pode se notar que houve uma grande evolução ao longo do tempo. A primeira lei sobre o tema foi a Lei nº 9.296/1996, que regulamentou a interceptação de comunicações telefônicas, após ela vieram outras leis importantes como a conhecida lei

Carolina Dieckmann Lei nº 12.737/2012 que representou um grande avanço na garantia da privacidade e proteção de informações pessoais no meio digital, definindo e criminalizando condutas como invasão de sistemas e acesso indevido a dados. O Marco Civil, Lei 12.965/2014, o qual estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil determinando as diretrizes para atuação dos entes federativos em relação a matéria, e por fim a mais recente Lei 14.155/2021, que inseriu e modificou artigos no Código Penal, majorando a pena destes crimes.

Desta forma, é visível que o Brasil possui leis que abordam o tema da cibercriminalidade, entretanto, é necessário a constante evolução das leis e incidência destas devido o grande desafio que o tema apresenta ao Estado, sendo necessário além de uma legislação abrangente e atualizada, outros três elementos essenciais para atingir esse objetivo: o avanço tecnológico, a educação digital e a colaboração internacional. A articulação internacional desempenha papel fundamental no enfrentamento e na prevenção dos crimes cibernéticos, considerando que muitos desses delitos transpassam fronteiras, dificultando a identificação e responsabilização dos infratores. Diante disso, é fundamental que os países unam esforços, promovendo o intercâmbio de informações, desenvolvendo políticas públicas conjuntas e firmando acordos de extradição.

2 REFERENCIAL TEÓRICO

Cotidianamente várias pessoas utilizam dos meios eletrônicos para buscar informações, conversar nas redes sociais, por videoconferência ou chamadas, executar operações bancárias e entre outras variadas maneiras. Entretanto, apesar das vantagens que o ambiente virtual fornece, como a celeridade e facilidade das ações, também foi estendida aos criminosos a possibilidade de cometer crimes, como por exemplo, furto, roubo, estelionato, difamação entre outros. Pois segundo Barbosa (2020), esses criminosos encontram na internet, uma maneira de se esconder “atrás” de um computador ou até mesmo acreditam que a punição para esse tipo de crimes acaba sendo menos severa do que deveria.

O crime cibernético, ou virtual, é definido como sendo qualquer atitude típica, ilícita e culpável que preenche os requisitos de infração penal, seja por dolo ou culpa, executado por pessoa física ou jurídica se utilizando da internet ou meio informático, que viole a segurança do sistema, a integridade e a privacidade dos indivíduos ou entidades (Marra, 2019, p. 153). As ações realizadas no ambiente virtual, quando motivadas por intenção

maliciosa e com o objetivo de prejudicar terceiros, podem provocar diversos tipos de danos às vítimas, muitas vezes irreversíveis. Isso inclui a divulgação de imagens sensíveis, fraudes que utilizam informações pessoais e bancárias obtidas de forma ilícita, enganos por meio de perfis falsos, promessas enganosas para enganar pessoas, e consequências devastadoras na vida de muitos, enquanto o autor se esconde atrás de uma tela (Goulart; Cordova, 2023, p..223).

O direito é regulador do comportamento humano em sociedade, em cada momento histórico e cultural de determinado povo, de modo que as normas se modificam com o passar do tempo. Desta maneira, com o advento da tecnologia e um mundo cada vez mais conectado, surgiram condutas contraditórias no mundo virtual, e da mesma maneira estas devem ser englobadas pelo ordenamento jurídico, visando promover segurança à sociedade. O Brasil avançou significativamente na legislação penal voltada para crimes digitais desde a implementação do Código Penal de 1940. Um marco importante nesse progresso foi a Lei 12.737/2012, conhecida como Lei Carolina Dieckmann que trata especificamente sobre esse tema, garantindo a privacidade e intimidade das pessoas, como por exemplo a não divulgação de imagens íntimas, fato esse que ocorreu com a atriz citada.

Além disso, houve também a introdução do Marco Civil da Internet Lei 12.965/2014. No que diz respeito ao Marco civil da Internet, este estabeleceu princípios, garantias, direitos e deveres para a utilização da internet no Brasil. Essa lei prevê que as redes sejam neutras, que os usuários tenham privacidade e os provedores responsabilidades. Assim, os usuários tiveram acesso a liberdade de expressão e acesso igualitário a informação, porque os provedores não mais podiam bloquear os conteúdos arbitrariamente. Além disso, também estabeleceu que direitos à privacidade dos usuários, exigindo que as empresas respeitassem seus dados pessoais. O Marco civil também estabeleceu ações que o estado deve adotar para a inclusão digital, fazendo com que o acesso à internet seja universal e possua uma infraestrutura de banda larga abrangente.

Ademais, a legislação regulamenta a retenção de registros de conexão, dando permissão de acesso a esses dados pelas autoridades em situações específicas, como por exemplo em investigações criminais, definindo limites para assegurar a privacidade dos usuários. Assim, essa legislação é fundamental que modificou a relação das pessoas com a internet. Esse avanço culminou com a criação da Lei 14.155/2021, que estabeleceu penas mais rigorosas para crimes cibernéticos como fraude, furto e estelionato, especialmente

quando cometidos através de dispositivos como celulares e computadores. A nova legislação substituiu o texto anterior, aumentando as penas para furto qualificado, invasão de dispositivo informático e crimes de estelionato digital (Freitas, Gonçalves e Torres 2023, p.307).

A necessidade de debates sobre os crimes cibernéticos é relevante porque existe hoje a migração dos criminosos para o ambiente virtual, e isso se sucede pois segundo Sydow: "tal categoria de crimes dispensa contato físico entre vítima e ofensor, não exige grandes preparos, como visitaç o pr via de local para cometimento do fato, ocorre em um ambiente sem povo, governo ou territ rio, n o implica aparentemente em altos riscos, n o gera sensa  o de viol ncia, e n o h  padr es para seu acontecimento". Pode-se dizer que o infrator se esconde na penumbra do anonimato que a tecnologia lhe proporciona e socorre-se da facilidade para perpetrar a infra  o penal (Goulart, Cordova, 2023, p g. 34).

Fabiane Marra (2019) conclui que o principal obst culo n o reside na legisla  o, j  que o Direito Penal continua a regular a sociedade por meio do poder estatal e a assegurar a prote  o social, promovendo a puni  o dos infratores. Assim, o maior desafio est  na pol tica de combate aos crimes digitais, pois enfrentamos a falta de profissionais qualificados e preparados para lidar com a nova realidade cibern tica. Esse despreparo   reflexo de um sistema deficiente e negligente.

A solu  o seria investir na melhoria e na qualifica  o desses profissionais para fortalecer a resposta a essas amea as (Freitas, Gonçalves e Torres, 2023, p.309). No Brasil, em 2024, uma pesquisa realizada pelo Instituto Nacional de Combate ao Cibercrime revelou que o pa s enfrentava uma escassez de 232 mil profissionais de ciberseguran a. No entanto, a situa  o pode ser ainda mais preocupante do que os dados indicam, uma vez que o Brasil tamb m lidera as demiss es globais no setor de Seguran a Cibern tica, com 38% dos entrevistados afirmando que suas empresas fizeram cortes nessa  rea.

Al m do  mbito da falta de profissionais na  rea de ciberseguran a, existe pouco investimento no setor, segundo a mesma pesquisa da INCC, quando se compara a Autoridade Nacional de Prote  o de Dados (ANPD), principal regulador federal sobre o tema no Brasil, obteve um or amento aproximado de R\$: 24 milh es para o ano de 2024, no ano anterior a Cybersecurity and Infrastructure Security Agency, principal regulador federal sobre o tema nos Estados Unidos, teve um or amento de US\$: 2.9 bilh es (cerca de R\$: 14 bilh es, em c mbio atual).

Atualmente com a alta conectividade que o ambiente virtual proporciona, se tornou uma prioridade mundial combater os ciberdelitos, sendo que o poder público exerce função primordial na prevenção e proteção contra esses atos. Deste modo, fica evidente a importância de quatro elementos para a concretização desse objetivo, são eles o investimento tecnológico, a educação digital, a cooperação internacional e por fim a criação de legislação abrangente (Maia e Costa, 2023 p.122). Em território nacional, cabe aos legisladores manterem nossas leis atualizadas e contextualizadas com o cenário digital atual, embora existam leis vigentes em nosso ordenamento jurídico a respeito do tema, cabe ao governo dar condições adequadas as forças policiais para que cada vez mais obtenham êxito nas investigações e captura dos criminosos, surtindo assim o efeito de repressão e prevenção dessa prática delitiva.

3 METODOLOGIA

A metodologia utilizada neste trabalho científico se fundamenta no método hipotético-dedutivo, o qual se caracteriza pela formulação de hipóteses com base na observação de um fato, seguido pela dedução lógica de consequências que serão testadas a partir de dados empíricos ou teóricos. No contexto do estudo, a hipótese inicial considerada é de que o avanço tecnológico, aliado à sensação de anonimato e à fragilidade das estruturas jurídicas e operacionais do Estado, contribui significativamente para o aumento da criminalidade no ambiente digital.

A partir dessa hipótese, adotou-se a revisão bibliográfica e documental como técnicas metodológicas para examinar a evolução da legislação brasileira, identificar os tipos de crimes cibernéticos mais comuns, e compreender os sujeitos envolvidos nessas práticas ilícitas. De modo que para embasar essa análise, o método da pesquisa bibliográfica foi realizado inicialmente por meio da leitura de artigos científicos, livros especializados, revistas digitais e outras fontes acadêmicas.

O material coletado foi selecionado e filtrado com base em sua relevância, atualidade e consistência teórica, sendo posteriormente organizado em uma tabela de fichamento contendo os trechos e citações mais pertinentes ao tema, o que garantiu maior sistematização e profundidade à investigação. Essa abordagem é adequada, pois permite estabelecer um raciocínio dedutivo: se os crimes cibernéticos se aproveitam da lacuna legislativa, da ineficiência investigativa e da escassez de profissionais qualificados, então é

possível concluir que o sistema jurídico atual precisa ser reestruturado para enfrentar tais desafios de forma eficaz.

Ao longo do estudo, demonstra-se que apesar de avanços normativos como a Lei nº 12.737/2012, o Marco Civil da Internet (Lei nº 12.965/2014) e a Lei nº 14.155/2021, o combate aos delitos virtuais ainda esbarra em fatores operacionais, como a falta de investimentos e de capacitação técnica. O método hipotético-dedutivo permite que se analise a relação entre o crescimento exponencial da conectividade e o surgimento de novas modalidades criminosas, como o furto eletrônico, a clonagem de cartões e a disseminação de malwares.

A partir disso, é possível deduzir que o ordenamento jurídico, por si só, não é suficiente se não for acompanhado de políticas públicas integradas, campanhas de conscientização digital e cooperação internacional. Além disso, o método adotado oferece sustentação lógica para a conclusão de que a criminalidade virtual não apenas reproduz crimes tradicionais em ambiente digital, mas também cria novas formas de ameaça à integridade de dados e à privacidade. Por fim, a utilização do método hipotético-dedutivo confere ao trabalho um caráter investigativo rigoroso e estruturado, que permite não só descrever, mas também propor soluções viáveis frente à complexidade dos crimes cibernéticos, destacando a necessidade de uma abordagem multidisciplinar e preventiva.

4 RESULTADOS ALCANÇADOS OU ESPERADOS

Embora o avanço tecnológico traga benefícios inquestionáveis, ele também exige uma resposta combativa aos novos desafios que surgem, em especial no que diz respeito aos crimes cibernéticos. Conclui-se, portanto, que o crime cibernético é aquele praticado valendo-se do uso de dispositivo eletrônico no ambiente virtual, se utilizando da internet ou não, que preencha os requisitos de uma atitude típica, ilícita e culpável. Dessa maneira, a legislação brasileira avançou consideravelmente com a publicação da Lei Carolina Dieckmann, o Marco Civil da Internet e as novas redações do Código Penal, mas ainda há um caminho longo a ser percorrido para garantir proteção efetiva aos cidadãos no ambiente virtual, devido este tipo de delito ser altamente mutável, sendo necessário a constante evolução da legislação, objetivando a transparência desta à sociedade e incidência sobre os indivíduos que cometem tais delitos.

Desta maneira, é imprescindível existência de uma ação conjunta entre o governo, empresas e a sociedade, de modo que trabalhem juntos para criar uma estrutura fortificada

que envolva desde a prevenção até a punição adequada para os criminosos. Sendo assim, faz-se necessário o investimento tecnológico, educacional, e a cooperação internacional para que esse objetivo se concretize, de modo essencial a existência de políticas públicas que colaborem para que os profissionais de cibersegurança, assim como os de segurança pública, recebam investimentos e sejam capacitados para o enfrentamento ao crime cibernético.

É preciso também a conscientização da população por meio da educação digital, para que possam prevenir-se e não fiquem vulneráveis a estas práticas delituosas, porque grande parte dos usuários de dispositivos digitais não possuem conhecimentos sobre as ferramentas que os rodeiam. Cerca de 60% dos usuários brasileiros não possuíam antivírus no celular e utilizavam redes de Wifi públicas, 47% utilizaram algum mecanismo, como JailBreak e Root, para burlar controles de segurança dos dispositivos, instalando aplicativos não-autorizados, ainda, 60% dos usuários não se atentam às permissões requeridas por um aplicativo (INCC, 2024, p.33), assim tornando-os mais vulneráveis pela simples falta de conhecimento sobre o tema.

Cabe ao estado a criação de campanhas educativas e informativas com a intenção de informar o público em geral para que haja uma autoproteção por parte da população, desestimulando e dificultando as práticas ilegais, de modo que a inexistência de uma educação digital abrangente corrobora para o agravamento das desigualdades sociais, comprometendo a formação profissional e ocasionando a marginalização destes indivíduos no ambiente virtual. A partir da implementação desses elementos supracitados, será possível a criação de um ambiente virtual mais seguro, garantindo que a inovação tecnológica seja utilizada para o progresso social e econômico, e não como uma ferramenta para práticas delituosas.

REFERÊNCIAS

BARBOSA, Mateus Israel Alves Crivinel. Crimes virtuais: a evolução dos crimes cibernéticos e os desafios no combate. 2020. 96 f. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Pontifícia Universidade Católica de Goiás, Goiânia, 2020. Disponível em: <https://repositorio.pucgoias.edu.br/jspui/handle/123456789/105>. Acesso em: 29 abr. 2025.

BRASIL. Lei nº 12.965, Marco Civil da Internet, de 23 de abril de 2014, disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.html

CRUZ, Diego; RODRIGUES, Juliana. Crimes cibernéticos e a falsa sensação de impunidade. Revista Científica Eletrônica do Curso de Direito, Garça, v. 13, n. 1, jan. 2018. Semestral. ISSN 2358-8551. Acesso em: 30 abr. 2025.

DA COSTA, Marco Aurélio Rodrigues. Crimes de informática. 1995. 22 f. Monografia (Graduação em Direito) – Pontifícia Universidade Católica do Rio Grande do Sul. Disponível em: <http://www.jus.com.br/doutrina/crinfo.html>. Acesso em: 29 abr. 2025.

DE FREITAS, Camila Cristina Gonzaga; GONÇALVES, Jonas Rodrigo; TORRES, Mateus Guimarães. A evolução do direito penal brasileiro relacionado aos crimes cibernéticos. REVISTA JRG DE ESTUDOS ACADÊMICOS, v. 6, n. 12, p. 296-311, 2023. Acesso em 30 abr. 2025

GARCIA, R. A. C.; CARUZO, W. R.; ZAMQUIM JUNIOR, J. W. Crimes cibernéticos. Revista Matiz Online, v. 01, p. 1–19, 2017. Disponível em:

<https://revista.matizonline.com.br/crimes-ciberneticos>. Acesso em: 29. abr. 2025.

GOULART, Luiz Carlos Shishito; CORDOVA, Maiko Giordani Santos. Ciberdelitos: uma análise jurídica dos crimes digitais. São Paulo: Dialética, p. 34;223. 2023.

INSTITUTO NACIONAL DE COMBATE AO CIBERCRIME (INCC). As contribuições para a estratégia nacional de cibersegurança. 2024. Disponível em: <https://incc.org.br/wp-content/uploads/2024/07/As-Contribuic%C3%A7%C3%83es-para-a-Estrate%C3%81gia-Nacional-de-Ciberseguranc%C3%A7a-INCC-2024.pdf>. Acesso em: 27 abr. 2025.

MAIA, Karolline Barbosa; COSTA, Cezar Henrique Ferreira. Crimes cibernéticos. Revista Ibero-Americana de Humanidades, Ciências e Educação, v. 9, n. 10, p. 109-126, 2023. Acesso em: 28 abr. 2025.

MARRA, Fabiane Barbosa. Desafios do direito na era da internet: uma breve análise sobre os crimes cibernéticos. Journal of Law and Sustainable Development, v. 7, n. 2, p. 145-167, 2019. Acesso em: 28 abr. 2025.

PENTEADO, Jacques de Camargo (Coord.) et al. Crimes de informática e investigação policial. In: _____. Justiça Penal, v. 7: Críticas e sugestões: justiça criminal moderna: proteção à vítima e à testemunha. São Paulo: Revista dos Tribunais, 2000. p. 317-318. Acesso em 29 abr. 2025.