PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
PRO-REITORIA DE GRADUAÇÃO
ESCOLA DE DIREITO, NEGÓCIOS E COMUNICAÇÃO
CURSO DE DIREITO
NÚCLEO DE PRÁTICA JURÍDICA
COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO

CRIMES CIBERNETICOS: DESAFIOS E PERSPECTIVAS NA ERA DIGITAL

ORIENTANDO – **PEDRO PAULO CUNHA XAVIER**

ORIENTADORA – PROFA. Dra. HELENA BEATRIZ DE MOURA BELLE

GOIÂNIA - GO
2025

PEDRO PAULO CUNHA XAVIER

CRIMES CIBERNETICOS:
DESAFIOS E PERSPECTIVAS NA ERA DIGITAL

Artigo apresentado à disciplina Trabalha de Curso II, da Escola de Direito, Negócios e Comunicação da Pontifícia Universidade Católica de Goiás (PUC GOIÁS), turma: A06. Profa. Orientadora Doutora Helena Beatriz de Moura Belle.

GOIÂNIA – GO
2025

PEDRO PAULO CUNHA XAVIER

CRIMES CIBERNETICOS:
DESAFIOS E PERSPECTIVAS NA ERA DIGITAL

Palavras chave: Cibercrime, Fraude Online, Segurança da informação, Proteção de Dados e Segurança de rede

Data da Defesa: _____ de _____de _____

BANCA EXAMINADORA

_____

Orientadora: Profa. Dra. Helena Beatriz de Moura Belle Nota

_____

Examinador(a) Convidado(a): Prof.(a): Titulação e Nome Completo Nota

CRIMES CIBERNETICOS: DESAFIOS E PERSPECTIVAS NA ERA DIGITAL

Resumo: O presente artigo realiza uma análise dos crimes cibernéticos e dos desafios que o ordenamento jurídico enfrenta na contemporaneidade digital. A rápida evolução das tecnologias e a crescente ubiquidade da internet fomentam novas modalidades de criminalidade, que incluem fraudes eletrônicas, roubo de dados, crimes financeiros e invasões de privacidade. Esses fenômenos exigem uma significativa adaptação dos dispositivos legais e das práticas judiciais existentes, que muitas vezes se mostram inadequados para lidar com a complexidade e a dinamicidade do ambiente digital. Um dos aspectos centrais da pesquisa é a tipificação penal dos crimes cibernéticos, que perpassa pela necessidade de uma definição clara e precisa das condutas ilícitas que ocorrem no contexto digital. A ambiguidade legislativa pode levar a dificuldades na inculpação e na responsabilização dos agentes infratores. Nesse contexto, é crucial analisar a complexidade das provas digitais, que são frequentemente voláteis e de difícil obtenção, além de requerer conhecimentos especializados que desafiam o tradicional entendimento forense. Outro ponto pertinente abordado neste estudo refere-se à responsabilidade civil e penal no ambiente cibernético. O crescente número de infrações exige uma reflexão sobre a responsabilidade das plataformas digitais, bem como dos provedores de serviços.

INTRODUÇÃO

Os crimes cibernéticos representam um dos maiores desafios contemporâneos para o sistema jurídico brasileiro, em razão da rápida evolução das tecnologias da informação e da comunicação, que transformam constantemente a dinâmica da sociedade e impõem novas demandas ao ordenamento jurídico. O ambiente digital, com suas especificidades, como a ausência de fronteiras físicas, a anonimização de ações e a natureza global das infrações, apresenta um contexto complexo e multifacetado que exige uma adaptação urgente e eficaz das normas legais. Nesse cenário, surge a necessidade de um tratamento jurídico mais robusto e específico para o enfrentamento dos crimes digitais, que vão desde a invasão de dispositivos eletrônicos até a utilização indevida de dados pessoais, sem esquecer as sofisticadas formas de fraude digital, ciberterrorismo e o impacto da inteligência artificial nas investigações criminais.

No Brasil, a legislação atual enfrenta grandes desafios para acompanhar a velocidade das inovações tecnológicas. Embora o Código Penal Brasileiro contemple alguns dispositivos que tratam de crimes cibernéticos, como os artigos 266 e 298, que abordam, respectivamente, a invasão de dispositivo eletrônico e a falsificação de

documentos digitais, essas disposições não são suficientes para abranger a totalidade das novas infrações que surgem no ambiente digital. Nesse contexto, destacam-se a Lei nº 12.737/2012, também conhecida como Lei Carolina Dieckmann, que tipificou a invasão de dispositivos eletrônicos, e a Lei nº 13.709/2018, a Lei Geral de Proteção de Dados Pessoais (LGPD), que estabelece requisitos rigorosos para o tratamento de dados pessoais e reforça a privacidade no meio digital.

No entanto, mesmo com essas legislações, o Brasil ainda enfrenta lacunas significativas no que diz respeito à regulamentação dos crimes cibernéticos. A legislação brasileira precisa evoluir, especialmente no tocante à regulação de crimes transnacionais, à utilização de provas digitais e à implementação de medidas que garantam a efetiva cooperação internacional no combate ao cibercrime.

Dentre os avanços legislativos recentes, o Projeto de Lei nº 2.013/2020, que visa a criação de um tipo penal específico para o uso indevido de dados pessoais, como o furto de dados (data theft), e o Projeto de Lei nº 3.261/2020, que propõe a regulamentação do uso de inteligência artificial nas investigações criminais e a facilitação da cooperação internacional, se destacam como tentativas de suprir as lacunas existentes e fortalecer o combate ao cibercrime no país.

O Brasil, além disso, participa ativamente das discussões internacionais sobre crimes cibernéticos, como as deliberações da Convenção de Budapeste sobre Cibercrime, buscando integrar-se de maneira mais eficaz às práticas globais de combate a esse fenômeno. A criação de um marco regulatório mais harmonizado, que permita a cooperação internacional e a padronização das normas legais sobre o tema, é essencial para aumentar a eficácia da repressão ao cibercrime e garantir a segurança jurídica em um ambiente cada vez mais digitalizado.

O objetivo deste trabalho é analisar os principais desafios enfrentados pelo direito penal brasileiro na tipificação, investigação e punição dos crimes cibernéticos, especialmente no que se refere à adaptação do ordenamento jurídico às novas tecnologias. A pesquisa irá abordar as lacunas normativas existentes, a validade e o tratamento das provas digitais, bem como as perspectivas de evolução legislativa, com ênfase nas propostas de reformas como o Projeto de Lei nº 2.013/2020 e o Projeto de Lei nº 3.261/2020. Além disso, será analisado o papel da jurisprudência, especialmente nas decisões do Supremo Tribunal Federal, e as possíveis soluções para aprimorar o sistema jurídico brasileiro frente aos desafios impostos pela cibercriminalidade.

1 INÍCIO DOS CRIMES CIBERNÉTICOS E SUA EVOLUÇÃO NO CENÁRIO ATUAL

Os crimes cibernéticos surgiram com o advento da internet e a crescente digitalização das atividades humanas. Na década de 1990, com a popularização da internet, começaram a aparecer os primeiros crimes digitais, inicialmente restritos a práticas como *hacking, spamming* e a distribuição de vírus. Esses crimes, inicialmente vistos como isolados e sem grande impacto, começaram a afetar não só indivíduos, mas também empresas e governos, tornando-se um fenômeno mais amplo e complexo. À medida que a tecnologia evoluía, novas modalidades criminosas surgiram, envolvendo fraudes financeiras, invasões de sistemas, roubo de dados pessoais e até o comprometimento de informações confidenciais de grandes corporações e instituições públicas. (Kerr, 2006)

O marco inicial na regulamentação dos crimes cibernéticos no Brasil foi a criação da Lei nº 12.737/2012 (Lei Carolina Dieckmann), que tipificou delitos como a invasão de dispositivos eletrônicos e a obtenção de informações de forma ilícita. Esta foi uma das primeiras tentativas de estabelecer um controle jurídico sobre o crescente problema dos crimes cibernéticos no país. No entanto, o fenômeno dos crimes cibernéticos é altamente dinâmico e acompanha o ritmo acelerado das inovações tecnológicas, o que torna a legislação frequentemente defasada. O Brasil também experimentou dificuldades para se adaptar às novas realidades digitais, o que refletiu na necessidade de regulamentações mais profundas e modernas.

Com o passar dos anos, os crimes cibernéticos se sofisticaram. A partir da década de 2010, a criminalidade digital passou a incluir delitos mais complexos, como fraudes bancárias eletrônicas, *ransomware*, crimes de identidade, ataques a sistemas críticos de infraestrutura e disseminação de fake news. O *ransomware*, por exemplo, se tornou um dos crimes cibernéticos mais alarmantes, no qual os criminosos sequestram dados de empresas ou indivíduos, criptografando-os e exigindo um resgate, geralmente em criptomoedas, para a liberação da informação. O uso crescente de criptomoedas e da dark web dificultou a atuação das autoridades, pois essas ferramentas permitem a anonimização dos criminosos e dificultam a

rastreabilidade das ações ilícitas, tornando as investigações ainda mais desafiadoras. (Wilson, 2017)

Além disso, com a crescente digitalização da sociedade, a utilização de plataformas online para transações financeiras, redes sociais e armazenamento de dados pessoais facilitou o surgimento de novas fraudes, como o phishing, que se tornou uma das técnicas mais comuns. A fraude digital, voltada para o roubo de dados sensíveis, explora a vulnerabilidade humana, enganando usuários a fornecerem informações como senhas e números de cartões de crédito. A atuação dos criminosos no ciberespaço tornou-se, assim, mais sofisticada e globalizada, pois, ao contrário dos crimes tradicionais, esses criminosos podem operar de qualquer lugar do mundo, o que amplia enormemente o alcance das infrações e os danos causados. Ataques a sistemas críticos de infraestrutura, como redes elétricas e hospitais, representaram riscos elevados à segurança nacional e impactaram diretamente a vida da população. (Kaplan, 2020)

A evolução dos crimes cibernéticos está intimamente ligada ao avanço tecnológico, o que exige constante atualização da legislação e das práticas judiciais. O Brasil, por exemplo, enfrentou grandes desafios para acompanhar essa evolução. A criação da Lei Geral de Proteção de Dados (LGPD), em 2018, foi um esforço para regular o uso de dados pessoais e proteger a privacidade dos cidadãos. Entretanto, o constante desenvolvimento de novas tecnologias, como inteligência artificial, internet das coisas (IoT) e criptomoedas, exige que o marco jurídico seja revisado e atualizado com frequência para lidar com as novas ameaças e desafios. A criação de novos tipos penais voltados para crimes digitais também tem sido tema de debate no Brasil e em outros países, pois a criminalidade digital é distinta da tradicional em vários aspectos, como sua transnacionalidade e a ausência de fronteiras físicas. Assim, a criminalização de novas práticas, como o uso indevido de informações pessoais ou o uso de bots para fraudes financeiras, precisa ser abordada em legislações mais modernas. (www.planalto.gov.br.)

Outro ponto relevante no combate aos crimes cibernéticos é a colaboração internacional. A globalização da internet significa que criminosos podem operar de qualquer parte do mundo, dificultando a identificação e punição das infrações. Por isso, é fundamental que os países estabeleçam acordos de cooperação jurídica internacional, como a Convenção de Budapeste sobre crimes cibernéticos, que foi adotada em 2001 pelo Conselho da Europa e visa harmonizar as legislações e facilitar

a colaboração entre as nações para combater esse tipo de crime. O avanço tecnológico, a utilização da dark web e a facilidade de se ocultar na rede exigem uma abordagem coordenada entre os países, visando o fortalecimento das investigações e a prevenção de crimes digitais.

Além disso, o Código Penal Brasileiro (Decreto-Lei nº 2.848/1940) possui dispositivos que podem ser aplicados no contexto dos crimes cibernéticos. O artigo 155, que trata do furto, por exemplo, pode ser utilizado em casos de furto de dados, especialmente no contexto de acessos não autorizados a sistemas ou dispositivos eletrônicos. O artigo 155, § 4º, do Código Penal, estabelece penas mais severas quando o furto é praticado com o uso de chave falsa, o que poderia ser interpretado também como uma analogia aos crimes praticados por hackers ou invasores digitais. (SILVA, 2018)

No Código Civil, a proteção dos dados pessoais e os danos causados por práticas fraudulentas digitais também encontram respaldo. O **artigo 186** do Código Civil Brasileiro, que trata do conceito de **dano**, pode ser aplicado em casos de **danos digitais** causados por crimes cibernéticos, já que a invasão de sistemas ou a violação de dados pessoais pode resultar em prejuízos significativos à vítima. O artigo 927, por sua vez, trata da responsabilidade civil, determinando que aquele que causar dano a outrem tem o dever de repará-lo, o que pode ser aplicado tanto às vítimas de crimes cibernéticos quanto às empresas responsáveis pela proteção dos dados de seus clientes. (LUCAS,2021)

À medida que novas tecnologias continuam a emergir, como a computação quântica e as inteligências artificiais autônomas, o cenário dos crimes cibernéticos tende a se tornar ainda mais complexo. A inteligência artificial pode ser utilizada por criminosos para criar ataques ainda mais sofisticados, como deepfakes, e a automação de fraudes pode se expandir rapidamente. As autoridades precisarão estar preparadas para lidar com essas novas ameaças, o que exigirá a implementação de tecnologias de ponta, a constante revisão das legislações e a capacitação de profissionais de segurança digital.

A educação digital e a conscientização pública também desempenham um papel importante na luta contra os crimes cibernéticos. A conscientização sobre as boas práticas de segurança online, o treinamento de profissionais da área de TI e a promoção da educação sobre a proteção de dados pessoais serão fundamentais para reduzir os riscos de se tornar vítima de crimes digitais. As organizações

também terão que investir em sistemas de segurança mais robustos e em protocolos que garantam a proteção de informações confidenciais, especialmente no caso de empresas e instituições financeiras.

Portanto, a atuação dos criminosos no ciberespaço, cada vez mais diversificada e sofisticada, impõe à sociedade a urgente necessidade de adaptação do sistema jurídico. A crescente interdependência global, associada à velocidade das inovações tecnológicas, exige um esforço contínuo para atualizar as legislações, implementar novas tecnologias de segurança e promover a colaboração internacional. A criação de marcos legais robustos, a utilização de tecnologias avançadas de proteção e a conscientização sobre os riscos cibernéticos são passos essenciais para mitigar os danos causados por esses crimes e proteger a sociedade de futuras ameaças. (www.planalto.gov.br)

1.1 COMPETÊNCIA LEGISLATIVA E PREVISÃO CONSTITUCIONAL NO ENFRENTAMENTO AOS CRIMES CIBERNÉTICOS

A competência para a criação de normas e políticas públicas voltadas ao combate aos crimes cibernéticos no Brasil está principalmente atribuída à União, que tem a responsabilidade de elaborar e implementar a legislação necessária para a repressão a esses delitos. Embora a Constituição Federal de 1988 não trate de maneira específica dos crimes cibernéticos, ela estabelece um conjunto de princípios e direitos fundamentais que servem de base para a regulamentação das infrações no ambiente digital, especialmente no que tange à proteção dos direitos individuais e à segurança pública.

No que tange aos crimes cibernéticos, o artigo 5º, inciso XXXV, da Constituição Federal, assegura o direito de acesso à justiça, o que implica a possibilidade de o Estado oferecer meios legais e procedimentais eficazes para a defesa dos cidadãos contra crimes digitais, como fraudes eletrônicas, roubo de dados, e ataques a sistemas críticos. Contudo, a Constituição não detalha de forma explícita as normas para o combate a esses crimes, ficando o papel de regulamentação e aplicação dessas normas nas mãos do legislador ordinário, sob a supervisão dos tribunais.

A competência para legislar sobre crimes cibernéticos também se alinha ao princípio da unidade do ordenamento jurídico, onde as normas federais, estaduais e municipais devem ser compatíveis com os princípios constitucionais e com os tratados internacionais ratificados pelo Brasil, como a Convenção de Budapeste sobre Cibercrime, que visa a harmonização das legislações nacionais no combate ao cibercrime. No contexto brasileiro, a Lei nº 12.737/2012 e a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados - LGPD) surgem como marcos normativos importantes na regulamentação de infrações digitais, como a invasão de dispositivos eletrônicos e a proteção de dados pessoais, respectivamente.

No que tange à responsabilidade penal e à execução da legislação sobre crimes cibernéticos, o processo de tipificação, investigação e julgamento segue os princípios da legalidade, da ampla defesa e do contraditório, conforme estabelecido pelo artigo 5º da Constituição. O Código Penal Brasileiro, embora ainda careça de uma regulamentação específica e robusta para crimes digitais, contém dispositivos que são frequentemente aplicados a casos envolvendo crimes cibernéticos, como os artigos 266 (invasão de dispositivo eletrônico) e 298 (falsificação de documentos eletrônicos). A aplicabilidade dessas normas, no entanto, gera discussões sobre a adequação e a evolução da tipificação penal no enfrentamento das novas modalidades criminosas.

Além disso, a tipificação e a aplicação das normas relativas aos crimes cibernéticos devem ser alinhadas com os princípios da proporcionalidade e da capacidade contributiva do sistema judicial. O legislador e os tribunais devem garantir que a aplicação das normas seja eficaz, sem que se torne uma medida desproporcional ou um obstáculo à proteção dos direitos dos cidadãos.

Em relação à responsabilidade civil, destaca-se a Lei Geral de Proteção de Dados (LGPD), que não só regula a proteção de dados pessoais, mas também estabelece sanções administrativas para as infrações digitais. A responsabilização das empresas e dos indivíduos que violam as normas de segurança cibernética, como o vazamento de dados ou o uso indevido de informações pessoais, é um dos pontos centrais na discussão sobre a aplicação da lei, trazendo à tona a necessidade de um sistema de responsabilização eficiente, com a devida proteção dos direitos do cidadão. (Masson, 2020)

O processo de investigação de crimes cibernéticos exige um controle adequado da coleta de provas, especialmente no que se refere às provas digitais, que são fundamentais para a caracterização do delito. A legislação processual penal brasileira,

em conjunto com o *Código de Processo Penal*, tem sido adaptada para o uso de tecnologias digitais nas investigações. Contudo, ainda há um grande debate sobre a eficácia e a necessidade de reformas, como a criação de tipos penais específicos para novas formas de cibercrime, como o *phishing* ou os ataques de *ransomware*. (FURLAN, 2019)

A competência legislativa para tratar de crimes cibernéticos, portanto, exige a atuação coordenada entre os entes federativos, o respeito à Constituição e aos direitos fundamentais, bem como a implementação de uma legislação moderna e eficaz no enfrentamento do fenômeno da criminalidade digital. O processo de adaptação do sistema jurídico brasileiro frente aos crimes cibernéticos passa por uma constante evolução, buscando um equilíbrio entre a proteção dos direitos individuais e a efetividade das medidas punitivas, sempre em conformidade com os princípios constitucionais e as necessidades da sociedade contemporânea.

Nesse sentido, o autor *Cleber Masson* afirma que "o direito penal deve se adaptar às novas realidades tecnológicas, uma vez que os crimes cibernéticos se desenvolvem a partir de práticas inovadoras e mutáveis". A adaptação da legislação penal e processual brasileira ao fenômeno dos crimes cibernéticos é, portanto, um processo contínuo, que exige uma constante revisão das normas e um esforço coordenado entre as autoridades nacionais e internacionais. O Brasil, por exemplo, é signatário da Convenção de Budapeste sobre Cibercrime, um tratado internacional que visa à harmonização das legislações penais e à cooperação entre países no combate a crimes digitais, o que reforça a importância de se manter uma legislação interna alinhada com os padrões globais. A competência para a criação de normas e políticas públicas voltadas ao combate aos crimes cibernéticos no Brasil está, em sua maioria, atribuída à União, conforme estabelecido no artigo 22 da Constituição Federal de 1988, que trata da competência privativa da União para legislar sobre diversas matérias, incluindo as relacionadas à segurança pública e ao direito penal. A Constituição, embora não trate de maneira específica dos crimes cibernéticos, assegura um conjunto de direitos fundamentais e princípios constitucionais que são essenciais para a regulamentação das infrações no ambiente digital. Estes direitos incluem a proteção da privacidade, da liberdade de comunicação e a garantia de um processo judicial justo, aspectos que são fundamentais no enfrentamento das infrações digitais, como fraudes eletrônicas, roubo de dados e ataques a sistemas críticos.

1.3 A EVOLUÇÃO DOS CRIMES CIBERNÉTICOS

A ascensão das redes sociais na década de 2000 trouxe novas oportunidades para os criminosos. O roubo de identidade e fraudes financeiras se tornaram mais comuns, com atacantes explorando informações pessoais compartilhadas nas plataformas sociais. Além disso, o cyberbullying e o assédio online emergiram como preocupações significativas, levando a debates sobre privacidade e segurança nas redes sociais.

Nos últimos anos, a evolução da tecnologia, incluindo a inteligência artificial e a computação em nuvem, tem permitido que os crimes cibernéticos se tornem ainda mais sofisticados. Os ataques de ransomware, que criptografam dados e exigem resgates, se tornaram uma das principais ameaças. Exemplos notáveis incluem o ataque de ransomware WannaCry em 2017, que afetou milhares de organizações em todo o mundo, e o ataque à Colonial Pipeline em 2021, que resultou em interrupções significativas nas operações de fornecimento de combustível nos EUA.

A evolução dos crimes cibernéticos reflete a transformação da internet ao longo das últimas décadas. À medida que a tecnologia avança, os criminosos se tornam mais criativos e sofisticados em suas abordagens, apresentando desafios constantes para usuários e autoridades. A educação e a conscientização sobre segurança cibernética, juntamente com legislações eficazes, são essenciais para proteger indivíduos e organizações contra as ameaças em constante evolução no mundo digital. A luta contra os crimes cibernéticos é um esforço contínuo que requer colaboração entre governos, empresas e a sociedade civil para garantir um ambiente online mais seguro. (RIGGIO,2020)

2. A NATUREZA DOS CRIMES CIBERNÉTICOS: TIPIFICAÇÃO E DESAFIOS

A tipificação penal dos crimes cibernéticos representa um dos maiores desafios no campo jurídico brasileiro, diante da evolução das tecnologias digitais e do impacto crescente da internet nas atividades cotidianas. O Código Penal Brasileiro, em sua versão original, não contemplava de forma direta as infrações praticadas no ambiente digital, o que gerou a necessidade de criação de normas mais específicas para lidar

com as novas modalidades criminosas que surgiram com o avanço da tecnologia. (2023)

Embora o direito penal brasileiro tenha avançado, leis específicas como a Lei nº 12.737/2012, tenham sido marcos importantes ao tipificar a invasão de dispositivos eletrônicos, outros marcos legislativos recentes também contribuem para o enfrentamento dos crimes cibernéticos. Um exemplo disso é a Lei nº 13.842/2019, que alterou a Lei nº 9.613/1998, que trata de crimes de lavagem de dinheiro. A alteração veio para incluir o uso de recursos cibernéticos, como as criptomoedas, para fins ilícitos, especialmente para crimes de lavagem de dinheiro, ocultação de ativos e financiamento de atividades criminosas.

Com a popularização das criptomoedas e o aumento das transações financeiras digitais, os criminosos passaram a utilizar as plataformas digitais para ocultar e transferir recursos de forma anônima, dificultando o rastreamento e a punição desses delitos. A Lei nº 13.842/2019 representa um avanço importante na tentativa de limitar a utilização dessas tecnologias para atividades criminosas, criando um ambiente mais seguro para as transações digitais. Essa alteração trouxe à tona a importância de legislações que integrem o uso de novas tecnologias no combate aos crimes financeiros digitais, estabelecendo responsabilidades para plataformas e instituições financeiras, obrigando-as a implementar medidas de segurança para prevenir abusos. (www.planalto.gov.br)

Além disso, o artigo 266 do Código Penal, que trata da falsificação de documentos, tem sido amplamente aplicado a crimes cibernéticos envolvendo fraudes digitais. Este artigo prevê pena de reclusão de dois a seis anos e multa para quem falsificar documentos com a intenção de enganar terceiros. Embora a legislação já trate da falsificação de documentos, a complexidade e a sofisticação das fraudes digitais, como as praticadas em ataques de phishing ou nas fraudes bancárias, tornam a aplicação desse dispositivo mais difícil e demandam novas tipificações específicas.

Por exemplo, o phishing, um tipo de fraude que envolve o envio de emails ou mensagens fraudulentas com o intuito de roubar dados sensíveis de usuários, pode ser penalizado com base no artigo 171 do Código Penal, que trata de estelionato. No entanto, a ausência de uma tipificação clara e específica para crimes como o phishing ainda gera dificuldades no processo de identificação e punição dos criminosos. Em vista disso, a necessidade de atualização da legislação é cada vez mais evidente, como exemplificado pelo Projeto de Lei nº 2.030/2020, que visa modificar o Código

Penal Brasileiro para tratar de forma mais eficiente dos crimes cibernéticos. (Silva,2020)

Outro marco importante é a Lei nº 13.709/2018, a Lei Geral de Proteção de Dados Pessoais (LGPD), que estabelece diretrizes para a coleta, o armazenamento e o tratamento de dados pessoais. A LGPD não apenas visa proteger a privacidade dos indivíduos, mas também impõe sanções severas a empresas e indivíduos que descumprirem as regras de segurança, como vazamento de dados pessoais. Esta legislação é fundamental para a proteção dos dados no contexto digital e tem um impacto direto no combate a crimes cibernéticos, como o roubo de dados e a violação da privacidade. A regulamentação da proteção de dados pessoais representa um passo significativo para a construção de um ambiente mais seguro para transações online e para a integridade das informações digitais. (www.planalto.gov.br)

Contudo, as legislações atuais ainda enfrentam desafios frente à constante evolução dos crimes digitais. O ransomware, que sequestra dados para extorsão, e outras fraudes tecnológicas estão em constante mutação, o que exige uma adaptação contínua da legislação. O Projeto de Lei nº 2.030/2020 tem como objetivo resolver essas lacunas, criando tipificações mais precisas para essas novas formas de criminalidade cibernética. A proposta inclui, por exemplo, a tipificação de crimes como o phishing, que ainda carecem de uma regulamentação específica.

Portanto, a tipificação penal dos crimes cibernéticos no Brasil está em um processo contínuo de evolução, buscando uma adequação entre o direito penal e a realidade digital. O sistema jurídico brasileiro tem demonstrado esforços significativos para se adaptar às novas ameaças, por meio de leis como a LGPD, a Lei nº 13.842/2019 e o Projeto de Lei nº 2.030/2020. No entanto, a constante inovação das tecnologias exige que a legislação seja constantemente atualizada, garantindo que os direitos dos cidadãos sejam preservados e que os criminosos cibernéticos sejam adequadamente punidos. A evolução dessa legislação será essencial para garantir a proteção de dados, a segurança de sistemas e a manutenção da confiança da sociedade no ambiente digital. (ZAFFARONI, 2018)

2.1 O FATO GERADOR NO DIREITO PENAL CIBERNÉTICO: A AÇÃO ILÍCITA NO CIBERESPAÇO

O fato gerador dos crimes cibernéticos no direito penal refere-se à conduta ilícita praticada no ciberespaço, que resulta na violação de normas legais e prejudica a integridade de sistemas informáticos ou a privacidade de indivíduos. Diferentemente dos crimes tradicionais, onde a materialidade do delito pode ser facilmente verificada, no âmbito cibernético o fato gerador está intimamente ligado ao uso de tecnologias da informação e à execução de atos ilícitos que, muitas vezes, deixam poucas ou nenhumas evidências físicas. Com isso, a tipificação desses crimes exige uma abordagem específica, considerando as peculiaridades e os desafios impostos pela natureza digital das infrações.

No contexto do direito penal, o fato gerador de um crime cibernético ocorre sempre que um agente utiliza a internet ou dispositivos tecnológicos para cometer atos ilegais, como fraudes financeiras, invasões de sistemas, disseminação de vírus ou roubo de dados. Essa dinâmica de violação digital de direitos e bens jurídicos exige um entendimento aprofundado sobre os fundamentos do direito penal, especialmente no que tange à aplicação de normas e à identificação de condutas criminosas. O autor André Gonçalves (2019), em sua obra *Direito Penal Cibernético*, afirma que "o ciberespaço é um ambiente em constante evolução, onde as infrações se tornam mais difíceis de detectar e de combater, exigindo, assim, uma revisão das estruturas normativas e judiciais."

O fato gerador no direito penal cibernético não está restrito à simples ação de acessar sistemas sem autorização, mas envolve também uma série de condutas que prejudicam o direito à privacidade, à segurança dos dados e até à própria ordem pública. De acordo com Fábio Ulhoa Coelho (2020), no livro *Direito Penal: Parte Geral*, a criminalização das condutas no ciberespaço deve ser baseada na proteção de bens jurídicos fundamentais, como a privacidade, a segurança da informação e a liberdade individual, que se estendem ao contexto digital, exigindo uma aplicação precisa das normas e das punições previstas no Código Penal.

Uma das dificuldades no enfrentamento dos crimes cibernéticos está justamente na natureza volúvel e anônima do ambiente digital. Isso implica que, muitas vezes, a evidência do crime não está presente de forma tangível, o que gera complexidade no processo de apuração e na caracterização do fato gerador. As provas digitais, muitas vezes, são difíceis de obter e de apresentar no processo judicial, uma vez que as ações ilícitas no ciberespaço podem ser mascaradas através de ferramentas como proxies, VPNs e criptografia. O autor Marcelo Semer (2021), em

Crimes Cibernéticos e a Efetividade do Direito Penal, destaca que "a ausência de provas físicas e a facilidade com que as ações podem ser encobertas tornam os crimes digitais um grande desafio para a justiça criminal."

Para Cleber Masson (2020), autor da obra *Crimes Cibernéticos: O Impacto do Uso de Tecnologia no Direito Penal*, a tipificação de crimes cibernéticos deveria se basear em uma abordagem "sistemática", levando em consideração os impactos sociais e econômicos desses crimes. Ele argumenta que a ação ilícita no ciberespaço pode afetar não apenas a vítima direta, mas também a coletividade, uma vez que um ataque a sistemas bancários, por exemplo, pode gerar uma crise de confiança em todo o sistema financeiro.

Além disso, a jurisprudência tem sido um instrumento crucial no enfrentamento dos desafios impostos pelo direito penal cibernético. A Corte Superior tem se adaptado à crescente importância das provas digitais e ao uso de tecnologias no processo de investigação. O Habeas Corpus nº 143.528 (STF, 2017) é um exemplo em que a Corte reconheceu a validade de provas obtidas a partir de interceptações de comunicações eletrônicas, confirmando que, em certos contextos, as provas digitais têm a mesma legitimidade das provas físicas. Para Luiz Flávio Gomes (2017), em *Direito Penal e Criminologia*, a validade das provas digitais reflete um amadurecimento do direito penal brasileiro frente à novas formas de criminalidade que surgem com a evolução da tecnologia.

Com a crescente globalização das infrações digitais, a atuação das autoridades judiciais e policiais no combate aos crimes cibernéticos também enfrenta desafios. O Marco Civil da Internet, embora fundamental para garantir os direitos de usuários, também introduz complexidades no que tange à proteção de dados pessoais e à responsabilização dos prestadores de serviços online. Renato opice Blum (2021), especialista em direito digital, comenta que a legislação internacional, como a Convenção de Budapeste sobre crimes cibernéticos, tem sido um importante marco para a cooperação internacional no enfrentamento de delitos digitais, mas que a aplicação de tratados internacionais no direito penal exige uma adaptação da legislação nacional para torná-la mais eficaz.

Nesse cenário, o Projeto de Lei nº 2.030/2020, que propõe alterações no Código Penal para a tipificação mais específica de crimes digitais, busca não apenas a adaptação da legislação, mas também o alinhamento com os avanços tecnológicos que têm impactado a sociedade globalmente.

Portanto, o fato gerador dos crimes cibernéticos no direito penal é a ação ilícita praticada no ambiente digital, sendo fundamental para a tipificação penal a adaptação contínua da legislação, a valorização das provas digitais e a cooperação internacional. O estudo e a aplicação das normas precisam ser mais dinâmicos e atualizados, visando à proteção dos direitos fundamentais de privacidade e segurança, ao mesmo tempo que se enfrenta de maneira eficaz os novos desafios impostos pela cibercriminalidade.

2.2 JURISPRUDÊNCIA E A APLICAÇÃO DO DIREITO PENAL DIGITAL

A evolução da jurisprudência no Brasil tem sido um fator chave para a adaptação do direito penal à crescente realidade digital, evidenciando um esforço contínuo da justiça brasileira para enfrentar os desafios apresentados pelos crimes cibernéticos. A interpretação das normas jurídicas e a aceitação das provas digitais têm sido fundamentais no processo de adaptação do sistema legal, tanto em termos de reconhecimento da validade das provas quanto no aspecto da análise da natureza transnacional dos delitos digitais.

No que tange às provas digitais, um dos maiores desafios no enfrentamento dos crimes cibernéticos, o Superior Tribunal de Justiça (STJ) tem consolidado uma postura firme de validação das evidências digitais, assegurando que essas provas, quando obtidas com o devido respeito aos direitos constitucionais, são legítimas e imprescindíveis para a investigação. Em um julgamento emblemático de 2019, no Habeas Corpus 534.370/SP, a Corte destacou a importância das provas digitais, como os registros de acesso a sistemas, e-mails e logs de comunicação, afirmando que tais elementos têm a mesma legitimidade das provas físicas tradicionais, desde que obtidas conforme os preceitos legais, ou seja, mediante autorização judicial e com a garantia do contraditório e da ampla defesa. (www.stf.jus.br)

Esse julgamento revela um avanço significativo na interpretação do direito penal em um contexto digital, reconhecendo a validade de provas obtidas em investigações cibernéticas. Essa postura é crucial, pois crimes cibernéticos, como o phishing, fraudes bancárias ou invasões de sistemas, muitas vezes deixam poucas evidências materiais tangíveis. Em um cenário onde os criminosos digitais operam de forma cada vez mais sofisticada, com o uso de criptografia, anonimato e ferramentas para ocultação da identidade, as evidências digitais desempenham um papel

essencial na elucidação de delitos e na identificação de responsáveis. (www.camara.leg.br)

No entanto, a aplicação do direito penal no enfrentamento de crimes cibernéticos não se limita à interpretação da legislação nacional. A natureza transnacional desses crimes exige que o juiz tenha uma visão global, uma vez que muitos delitos digitais não se restringem a uma única jurisdição. Esse fenômeno exige que os sistemas legais de diferentes países cooperem entre si para garantir a investigação e a punição de delitos que, frequentemente, envolvem diversas fronteiras, recursos internacionais e tecnologias de difícil rastreamento.

Cleber Masson (2020), em sua obra *Crimes Cibernéticos: O Impacto do Uso de Tecnologia no Direito Penal*, argumenta que a crescente globalização dos crimes digitais exige um sistema legal que, além de estar alinhado com as normas internacionais, seja capaz de responder rapidamente às inovações tecnológicas que impactam as infrações cibernéticas.

Outro aspecto relevante na aplicação do direito penal aos crimes cibernéticos diz respeito à capacitação técnica dos magistrados. Os crimes digitais não se enquadram facilmente nas categorias tradicionais do direito penal, e muitas vezes exigem do juiz uma compreensão aprofundada das tecnologias envolvidas. Isso não significa que o juiz precise ser um especialista em tecnologia, mas sim que ele deve ser capaz de entender as implicações dos atos realizados no ciberespaço e como eles afetam os bens jurídicos protegidos, como a privacidade, a segurança dos dados e a integridade de sistemas. (Masson, 2020)

Para isso, o Estado brasileiro, assim como outros países, tem investido na formação de juízes especializados em crimes cibernéticos, oferecendo cursos de atualização e capacitação sobre o uso de provas digitais e as novas tecnologias aplicadas aos delitos. Além disso, a própria evolução do sistema jurídico, que tem incorporado a análise de provas digitais de forma mais sistemática, exige um esforço conjunto entre tribunais, Ministério Público e advogados para garantir uma resposta eficaz e proporcional às infrações cometidas no ciberespaço.

A crescente sofisticação dos crimes digitais apresenta novos desafios para o direito penal. Com o avanço das criptomoedas, a dark web e o uso de tecnologias de anonimização, muitos criminosos têm encontrado formas mais eficientes de realizar delitos sem deixar rastros, tornando a aplicação da lei ainda mais desafiadora. Além disso, com o surgimento de novas tecnologias, como a inteligência artificial e o uso de

blockchain, novas formas de crimes cibernéticos podem surgir, exigindo não apenas a criação de novas normas legais, mas também uma constante adaptação da jurisprudência. (Ribeiro, 2020)

3. O USO DA INTELIGÊNCIA ARTIFICIAL PARA O ENFRENTAMENTO DOS CRIMES CIBERNÉTICOS

A IA pode analisar grandes volumes de dados em tempo real, permitindo a identificação de padrões e comportamentos anômalos que podem indicar uma ameaça. Algoritmos de aprendizado de máquina são treinados para reconhecer o que é considerado "normal" em uma rede ou sistema, podendo, assim, detectar atividades suspeitas, como tentativas de invasão ou tráfego malicioso. (2025)

Sistemas de IA podem automatizar a resposta a incidentes de segurança. Uma vez que uma ameaça é identificada, a IA pode tomar medidas imediatas, como isolar um dispositivo comprometido, bloquear endereços IP suspeitos ou aplicar atualizações de segurança. Isso reduz o tempo de resposta e minimiza os danos potenciais. (2024)

A IA é utilizada para realizar análises de vulnerabilidades em sistemas e redes. Ferramentas de segurança baseadas em IA podem identificar fraquezas de segurança antes que possam ser exploradas por atacantes. Isso inclui a realização de testes de penetração automatizados, que simulam ataques para descobrir pontos fracos. Com o uso de algoritmos preditivos, a IA pode ajudar as organizações a antecipar possíveis ataques cibernéticos. Analisando dados históricos e tendências, os sistemas podem prever quais tipos de ataques são mais prováveis e sugerir medidas proativas de defesa.

Embora a IA ofereça muitos benefícios na segurança cibernética, também apresenta desafios. A dependência excessiva de sistemas automatizados pode resultar em falhas se não forem bem treinados ou se ocorrerem falsos positivos. Além disso, a utilização de IA por cibercriminosos para desenvolver ataques mais sofisticados é uma preocupação crescente. É crucial que as organizações implementem uma abordagem equilibrada, combinando tecnologia com a expertise humana.

A integração da inteligência artificial na segurança cibernética está transformando a forma como as organizações protegem seus sistemas e dados. Com a capacidade de detectar, responder e prever ameaças de maneira mais eficaz, a IA se tornou uma aliada indispensável na luta contra crimes cibernéticos. No entanto, à medida que essa tecnologia avança, é fundamental que as organizações permaneçam vigilantes e éticas, garantindo que as soluções de IA sejam utilizadas de forma responsável e eficaz. (www.ponemon.org)

CONSIDERAÇÕES FINAIS

O estudo dos crimes cibernéticos à luz do Direito Penal revelou uma realidade jurídica em constante transformação, impulsionada pela evolução das tecnologias digitais e pela crescente dependência da internet nas relações sociais e econômicas. Observou-se que o ordenamento jurídico penal brasileiro tem buscado responder às novas formas de criminalidade virtual, ainda que enfrente desafios significativos no processo de adaptação.

A tipificação penal de condutas praticadas no ambiente digital exige não apenas uma atualização legislativa constante, mas também um esforço interpretativo para compatibilizar os princípios do Direito Penal com as particularidades do ciberespaço. A dificuldade de identificação dos autores, a volatilidade das provas e a transnacionalidade das ações criminosas são apenas alguns dos fatores que impõem limites à atuação do Estado.

Embora leis específicas, como a que tipifica a invasão de dispositivos eletrônicos (Lei nº 12.737/2012) e o Marco Civil da Internet, tenham representado avanços importantes, é necessário reconhecer que o enfrentamento efetivo dos crimes cibernéticos exige uma abordagem mais abrangente. Isso inclui a capacitação de agentes públicos, o uso de tecnologias apropriadas na investigação criminal e, sobretudo, a promoção de parcerias internacionais que permitam a persecução penal além das fronteiras nacionais.

Em síntese, o Direito Penal deve continuar evoluindo para enfrentar a criminalidade digital de forma proporcional, eficaz e respeitosa aos direitos fundamentais. A construção de um sistema jurídico que responda adequadamente aos delitos praticados no meio digital depende do equilíbrio entre a repressão legal e a proteção das garantias constitucionais, reafirmando a função do Direito Penal como último recurso na defesa dos bens jurídicos mais relevantes da sociedade.

CYBERCRIMES: CHALLENGES AND PERSPECTIVES IN THE DIGITAL ERA

ABSTRACT

This article presents an analysis of cybercrime and the challenges faced by the legal system in the current digital age. The rapid advancement of technology and the increasing ubiquity of the internet foster new forms of criminal activity, including electronic fraud, data theft, financial crimes, and invasions of privacy. These phenomena demand significant adaptations of existing legal frameworks and judicial practices, which often prove inadequate for addressing the complexity and dynamism of the digital environment. A central aspect of the research is the criminal classification of cybercrimes, which involves the need for clear and precise definitions of illicit conduct occurring in the digital context. Legislative ambiguity can result in difficulties in prosecuting and holding offenders accountable. In this context, it is crucial to analyze the complexity of digital evidence, which is often volatile and difficult to obtain, and requires specialized knowledge that challenges traditional forensic understanding. Another relevant point addressed in this study concerns civil and criminal liability in cyberspace. The growing number of infractions calls for reflection on the responsibility of digital platforms as well as service providers.

Keywords: Cybercrime, Online Fraud, Information Security, Unauthorized Access and Data Protection

REFERÊNCIAS

ALMEIDA, João. Cibersegurança e Proteção de Dados na Era Digital. Editora Atlas, 2024.

BARBOSA, Luísa. Crimes Cibernéticos no Brasil: Desafios e Avanços Recentes. Editora Juspodivm, 2023.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Altera o Código Penal para tipificar o crime de invasão de dispositivo informático, entre outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2012/l12737.htm. Acesso em: 02 nov. 2024.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Institui o Marco Civil da Internet. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l12965.htm. Acesso em: 31 out. 2024.

BRASIL. Projeto de Lei nº 2.030, de 27 de maio de 2020. Altera a Lei nº 9.296, de 24 de julho de 1996, para possibilitar a interceptação de comunicações telemáticas, entre outras medidas de combate aos crimes cibernéticos. Disponível em: https://www.camara.leg.br/propostas-legislativas/2240052. Acesso em: 02 nov. 2024.

CARVALHO, Pedro. Investigação Digital e Provas Eletrônicas em Processos Criminais. Editora Saraiva, 2025.

CONSELHO DA EUROPA. Convenção sobre Cibercrime. Disponível em: https://www.coe.int/pt/web/conventions/full-list/-/conventions/treaty/185. Acesso em: 02 nov. 2024.

COSTA, Ana. Privacidade e Segurança da Informação: Estudos Avançados. Editora Forense, 2024.

DIAS, Ricardo. Fraudes Online e Medidas de Prevenção. Editora Lumen Juris, 2023.

FERREIRA, Mariana. A Interseção entre Direito Penal e Tecnologia. Editora Malheiros, 2024.

GONÇALVES, Lucas. Direito Digital e Cibercrimes: Uma Abordagem Contemporânea. Editora Método, 2023.

MARTIN, Jean. Crimes Cibernéticos: Aspectos Penais e Processuais. São Paulo: Editora Revista dos Tribunais, 2020.

MENDES, Carla. Responsabilidade Penal por Crimes Cibernéticos. Editora Almedina, 2023.

SAFFON, Ana Paula. A Regulação dos Crimes Cibernéticos no Brasil. Rio de Janeiro: Editora Forense, 2021.

SILVA, Bruno. Cibersegurança: Técnicas e Estratégias de Defesa. Editora Novatec, 2024.

SOUZA, Camila. Crimes Cibernéticos e a Proteção dos Direitos Fundamentais. Editora Juruá, 2025.

VENOSA, Silvio de Salvo. *Direito Penal, Parte Geral. 18. ed. São Paulo: Editora Atlas, 2021.