JNT - FACIT BUSINESS AND TECHNOLOGY JOURNAL - ISSN: 2526-4281 - QUALIS B1
ANO 2025 – MÊS DE MAIO - FLUXO CONTÍNUO – Ed. 62. Vol. 2. Págs. 187-206
DOI: 10.5281/zenodo.15530129

CRIMINALIDADE DIGITAL: DESAFIOS LEGAIS NO ENFRENTAMENTO

DIGITAL CRIME: LEGAL CHALLENGES IN CONFRONTING IT

João Miguel Soares de OLIVEIRA
Centro Universitário Tocantinense Presidente Antônio Carlos (UNITPAC)
E-mail: joao.bill.miguel@gmail.com
ORCID: http://orcid.org/0009-0007-7848-9300

Mainardo Filho Paes da SILVA
Centro Universitário Tocantinense Presidente Antônio Carlos (UNITPAC)
E-mail: mainardoadv@hotmail.com
ORCID: http://orcid.org/0009-0009-0919-4781

RESUMO

A criminalidade digital constitui um dos maiores desafios enfrentados pelos sistemas jurídicos contemporâneos. Com a expansão da *internet* e o avanço das tecnologias da informação, surgiram novas formas de delitos praticados no ambiente virtual, exigindo respostas adequadas do ordenamento jurídico. Este trabalho tem como objetivo analisar os principais obstáculos enfrentados no combate à criminalidade virtual, abordando desde a dificuldade de identificação e rastreamento dos criminosos até as limitações legislativas, a complexidade da cooperação internacional e a insuficiência de capacitação técnica dos agentes públicos. Por meio de revisão bibliográfica e análise legislativa, busca-se compreender as fragilidades do sistema atual e apontar caminhos para o seu aprimoramento. Os resultados evidenciam a necessidade de atualização normativa, maior investimento em recursos humanos e tecnológicos, e fortalecimento da cooperação jurídica entre os países.

Palavras-chave: Capacitação Técnica. Cooperação. Crimes Virtuais. Criminalidade digital. Legislação. Internacional.

ABSTRACT

Digital crime is one of the greatest challenges faced by contemporary legal systems. With the expansion of the internet and the advancement of information technologies, new forms of criminal offenses have emerged in the virtual environment, requiring adequate legal responses. This study aims to analyze the main obstacles in combating

digital crime, addressing issues such as the difficulty in identifying and tracking criminals, legislative limitations, the complexity of international cooperation, and the insufficient technical training of public agents. Through bibliographic review and legislative analysis, this research seeks to understand the current system's weaknesses and suggest improvements. The findings highlight the need for regulatory updates, greater investment in human and technological resources, and strengthened international legal cooperation.

Keywords: Technical Training. Cooperation. Cybercrimes. Digital Crime. Legislation. International.

INTRODUÇÃO

A era digital provocou transformações significativas em todos os setores da sociedade, impactando diretamente as relações sociais, econômicas, políticas e jurídicas. A incorporação da tecnologia no cotidiano, por meio da *internet*, redes sociais, plataformas digitais e dispositivos móveis, proporcionou benefícios indiscutíveis, como a democratização do acesso à informação, a ampliação da comunicação global e a dinamização da economia. Contudo, paralelamente ao avanço tecnológico, emergiram novas formas de criminalidade que se valem do meio digital como instrumento ou ambiente para a prática de delitos.

A criminalidade digital, também conhecida como cibercriminalidade, representa um dos grandes desafios do século XXI. Tais crimes se caracterizam por sua complexidade, pela rapidez de execução, pela facilidade de anonimato dos autores e, principalmente, pela transnacionalidade, que dificulta as investigações e a responsabilização penal. Casos de invasões de dispositivos eletrônicos, fraudes bancárias, disseminação de *malwares, ransomwares,* extorsões e crimes contra a honra na *internet* tornaram-se cada vez mais frequentes e sofisticados, exigindo uma nova postura do ordenamento jurídico.

Nesse contexto, o Direito enfrenta dificuldades significativas para se adaptar a essa nova realidade. As legislações nacionais muitas vezes são insuficientes para tipificar condutas virtuais emergentes, e a aplicação das normas tradicionais se mostra limitada diante das peculiaridades do ambiente digital. Além disso, a atuação

dos órgãos de segurança pública e do Judiciário encontra entraves operacionais, como a falta de estrutura tecnológica e a carência de profissionais especializados.

Este trabalho tem como objetivo central analisar os principais obstáculos enfrentados pelo sistema jurídico brasileiro no combate à criminalidade digital. A pesquisa se concentra em quatro eixos fundamentais: (1) a dificuldade de identificação e rastreamento dos criminosos, (2) as limitações legislativas, (3) os desafios da cooperação internacional e da jurisdição em crimes transnacionais, e (4) a capacitação técnica dos agentes públicos responsáveis pela repressão a esses delitos.

A relevância do tema se dá não apenas pela crescente incidência de crimes virtuais, mas também pela urgência de se construir mecanismos eficazes de prevenção, investigação e punição, de modo a assegurar os direitos fundamentais dos cidadãos no ambiente digital. A metodologia adotada inclui revisão bibliográfica, análise doutrinária e legislativa, com o intuito de propor reflexões e possíveis soluções para o aprimoramento do enfrentamento à criminalidade digital no Brasil.

CONCEITOS E CLASSIFICAÇÃO DOS CRIMES VIRTUAIS

O Que são Crimes Virtuais

Crimes virtuais são fenômeno que se intensificou com a crescente informatização da vida social, econômica e institucional, tem se tornado uma das maiores preocupações no campo da segurança pública e do direito. Com a massificação da *internet* e a popularização de dispositivos conectados em rede, surgiram novas formas de violação de direitos, praticadas de maneira digital, o que alterou profundamente o cenário tradicional de crimes.

Também conhecidos como crimes cibernéticos, referem-se a condutas ilícitas realizadas por meio de sistemas informatizados, geralmente no ambiente da *internet*. A Organização para Cooperação e Desenvolvimento Econômico das Nações Unidas (OCDE), no ano de 1983, deu se a definição para crime cibernético “qualquer conduta ilegal, antiética ou não autorizada que envolva processamento ou transmissão automática de dados” (Palazz, 2000, apud Fiorillo; Conte, 2016, p. 186). Logo, o crime virtual pode envolver o uso de tecnologias digitais para a prática do delito ou apenas

a utilização do meio digital para potencializar práticas criminosas já existentes no mundo físico.

Tal transformação da criminalidade traz à tona um cenário complexo, pois os crimes cibernéticos podendo afetar diversos aspectos da sociedade. Eles não se limitam à violação de dados ou ao comprometimento de sistemas de segurança, mas também atingem diretamente os indivíduos e as instituições. O espectro de impactos dessas infrações é vasto, podendo causar danos econômicos, psicológicos e sociais. Tais ações criminosas podem envolver a invasão de sistemas de computadores, a disseminação de *softwares* maliciosos (*malwares* e *ransomwares*), a fraude eletrônica, entre outros tipos de infrações que utilizam a rede digital como meio para sua execução.

"É de se imaginar que a existência de um local "seguro" onde é possível trafegar de forma anônima e de difícil localização se tornou atrativo para práticas criminosas. " (Santana Silva, 2016, p. 4). A vastidão da *internet* e o anonimato que ela proporciona são aspectos que tornam os crimes virtuais mais atraentes para os criminosos. Tais fatores tornam a investigação mais desafiadora e criam uma sensação de impunidade, uma vez que o criminoso pode se esconder atrás de interfaces digitais, dificultando a identificação e o rastreamento.

A rapidez com que as informações circulam na *internet* também contribui para o agravamento desse problema, permitindo que o crime se propague com uma velocidade muito maior do que seria possível em um contexto tradicional.

A criminalidade digital, portanto, exige uma abordagem multidisciplinar, que envolva tanto aspectos técnicos quanto jurídicos e sociais. Não é apenas uma questão de atualizar as leis ou de reforçar os sistemas de segurança digital, mas também de educar a sociedade para o uso responsável da tecnologia e de criar mecanismos de prevenção que envolvam todos os setores da sociedade, desde os indivíduos até as grandes corporações e os governos.

A rápida evolução da tecnologia exige que as medidas de combate à criminalidade digital se adaptem constantemente, e as leis existentes nem sempre acompanham o ritmo das inovações tecnológicas, o que dificulta o trabalho dos órgãos de justiça e de segurança pública.

Assim, o estudo dos crimes cibernéticos e da criminalidade virtual não pode se limitar a uma análise técnica ou jurídica, mas precisa levar em conta a interação entre

as tecnologias digitais e os comportamentos humanos, refletindo a complexidade desse fenômeno que transcende as fronteiras tradicionais do direito e da criminologia.

Classificações dos Crimes Cibernéticos

Os crimes cibernéticos podem ser classificados de acordo com a forma como se relacionam com a tecnologia digital e o ambiente virtual. É fundamental para compreender as especificidades de cada tipo de infração e suas implicações legais. Tiramos como exemplo as três categorias principais: crimes cibernéticos puros, crimes cibernéticos mistos e crimes tradicionais com apoio da tecnologia.

Vejamos:

> Essas classificações são eficazes didaticamente para se entender e classificar alguns crimes, mas por conta da rapidez na evolução e dinâmica da rede de computadores e internet fica quase impossível acompanhar e afirmar categoricamente que não há modalidades que não estejam elencadas nas classificações adotadas. (Almeida; Mendonça; Do Carmos; Santos; Silva; De Azevedo, 2015, p. 11).

O crime cibernético puro diz respeito a ações ilícitas com o propósito direto de comprometer sistemas computacionais, atingindo tanto o hardware quanto o software e os dados neles contidos, como ocorre em casos de invasão de servidores ou sites (Matsuyama; Lima, 2015). Exemplos típicos incluem a invasão de sistemas informáticos, disseminação de vírus e *malwares*, ataques de negação de serviço (DDoS) e roubo de identidade digital. Tais crimes geralmente têm como alvo empresas, instituições financeiras, governos ou indivíduos, causando danos financeiros, prejuízos à reputação ou comprometendo a privacidade das vítimas.

A dinâmica desses delitos exige que as leis acompanhem rapidamente a evolução tecnológica para assegurar que a legislação esteja sempre atualizada em relação às novas ameaças que surgem no ambiente digital.

Já os crimes cibernéticos mistos são caracterizados pelo uso da tecnologia como meio para a execução de delitos que, tradicionalmente, não dependem do ambiente digital para ocorrer. No caso do crime cibernético misto, o sistema informático não é o alvo direto da conduta criminosa, mas sim um meio essencial para a prática do delito, que visa atingir outros bens jurídicos, como ocorre em fraudes bancárias realizadas por meio do homebanking (Matsuyama; Lima, 2015). Nestes casos, o

ciberespaço é utilizado como ferramenta para facilitar a prática de crimes já existentes no mundo físico. Entre os exemplos mais comuns estão o estelionato eletrônico, a extorsão, a chantagem, e os crimes de falsidade ideológica.

O *phishing*, por exemplo, é uma prática bastante difundida que envolve o envio de mensagens fraudulentas com a intenção de obter dados sensíveis, como números de cartão de crédito, senhas bancárias e informações pessoais. Além disso, as redes sociais se tornaram plataformas propícias para a propagação de golpes, como o falso empréstimo *online*, onde criminosos se aproveitam da confiança dos usuários para aplicar fraudes financeiras. Esses crimes exigem uma abordagem mais flexível da legislação, que deve ser capaz de distinguir entre as formas tradicionais de criminalidade e suas versões digitais.

Podemos falar sobre os crimes tradicionais com apoio da tecnologia, que são aqueles que, embora conhecidos desde tempos anteriores à popularização da *internet*, passaram a ser organizados ou facilitados por meio da utilização de tecnologias digitais.

Vejamos:

> Atividade delitiva englobando qualquer ato criminoso relacionado aos computadores e/ou redes computacionais, inclusive "hacking". Os crimes cibernéticos também abrangem os crimes tradicionais, só que perpetrados nos novo ambientes de redes, o da Internet inclusive (Ferro Júnior; Lima, 2013, p. 24).

Um exemplo claro desse tipo de crime é o tráfico de drogas, que, com o advento de aplicativos de mensagens e plataformas de venda *online*, tornou-se mais difícil de rastrear e combater. Outros exemplos incluem o aliciamento de menores através de redes sociais e a lavagem de dinheiro utilizando criptomoedas. Esses crimes apresentam um grande desafio para as autoridades, pois a tecnologia facilita a realização de atos ilícitos de forma mais rápida, secreta e, muitas vezes, transnacional.

A natureza descentralizada da *internet* e o anonimato proporcionado por algumas plataformas digitais dificultam o trabalho das forças de segurança, exigindo uma maior cooperação internacional e estratégias mais robustas de monitoramento.

Entendendo as diferentes categorias e suas particularidades, podemos adaptar as abordagens, seja na aplicação das leis existentes ou na criação de novas normativas, para garantir uma resposta eficaz aos desafios impostos pela criminalidade digital. Além disso, a distinção entre essas categorias auxilia na

definição das competências jurisdicionais, permitindo que as autoridades identifiquem com mais precisão quais são as esferas responsáveis pelo julgamento dos crimes cibernéticos e quais são os recursos necessários para a investigação e repressão desses atos.

Principais Crimes Virtuais

Nossa legislação contempla diversas condutas criminosas praticadas por meios eletrônicos, acompanhando a crescente criminalidade digital e buscando garantir a proteção dos direitos dos cidadãos no ambiente virtual. Entre as infrações mais recorrentes, destacam-se, primeiramente, a invasão de dispositivo informático, tipificada pela Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann. Essa lei criminaliza o acesso não autorizado a sistemas informáticos com a intenção de obter, adulterar ou destruir dados.

O hacking configura-se como um crime cibernético de grande gravidade, caracterizado pela invasão não autorizada de sistemas computacionais, redes ou dispositivos (Maia; Costa, 2023). Essa prática, que demanda medidas de segurança sofisticadas e respostas rápidas, é realizada por indivíduos com habilidades técnicas avançadas, os quais, muitas vezes, visam obter lucro, praticar espionagem ou simplesmente demonstrar sua capacidade técnica. A invasão de dispositivos é uma prática comum em casos de *hacking*, onde indivíduos ou grupos buscam acessar informações privadas ou confidenciais, seja de usuários individuais ou de organizações. A Lei Carolina Dieckmann foi de suma importância, pois foi a primeira a tipificar de forma clara crimes cibernéticos no Brasil, reconhecendo a necessidade de uma abordagem mais específica para lidar com as infrações digitais.

Outrora, o crime de estelionato eletrônico é de grande recorrência, previsto no art. 171, §2º-A, do Código Penal Brasileiro, que trata da fraude praticada por meio de comunicação eletrônica.

De acordo com Toffolo Hoffelder e Castro (2018), com a constante evolução da tecnologia e da internet, surgem novos tipos de crimes, o que leva à reflexão sobre a necessidade de uma tipificação legal específica para o estelionato eletrônico. Esse tipo de fraude pode ocorrer por diversos meios, como a criação de sites falsos para enganar consumidores ou o envio de e-mails fraudulentos *(phishing)* para obter dados financeiros e bancários das vítimas. O estelionato eletrônico tem crescido

significativamente, especialmente com a popularização das transações financeiras digitais, sendo uma das infrações mais comuns na atualidade. A pena estipulada para este crime é de reclusão de 1 a 5 anos, além de multa, podendo ser aumentada dependendo da gravidade da fraude e do prejuízo causado à vítima.

O furto mediante fraude eletrônica é outra modalidade que se vale da tecnologia para enganar e subtrair bens ou valores das vítimas. Esse tipo de crime ocorre quando criminosos utilizam meios digitais para realizar fraudes, como o uso de falsos sistemas de pagamento ou de plataformas para transações *online*. A tecnologia facilita a execução desse tipo de furto, tornando-o mais difícil de ser detectado. O furto eletrônico se alinha ao conceito tradicional de furto patrimonial, mas com a peculiaridade de utilizar a tecnologia para enganar e obter vantagem ilícita.

Em relação aos *malwares* e *ransomwares*, essas são formas sofisticadas de crimes cibernéticos que envolvem a disseminação de *softwares* maliciosos. Os *malwares* são programas projetados para danificar ou tomar controle de dispositivos, enquanto os *ransomwares* bloqueiam o acesso a dados ou sistemas, exigindo o pagamento de resgate para liberá-los.

O *ransomware* tem se tornado um dos crimes mais preocupantes no cenário digital, afetando tanto indivíduos quanto empresas, que podem ser obrigados a pagar grandes quantias para recuperar seus dados. Em muitos casos, o pagamento é feito através de criptomoedas, o que dificulta o rastreamento e a identificação dos criminosos.

Mais um crime relevante no contexto digital é a divulgação não autorizada de imagens íntimas, também conhecida como "*revenge porn*". Essa prática consiste na divulgação de vídeos ou fotos íntimas sem o consentimento da pessoa envolvida, com a intenção de prejudicar sua honra, dignidade ou intimidade.

No ano de 2018, a Lei nº 13.718/2018 foi sancionada, tipificando a divulgação não autorizada de imagens íntimas como crime, com pena de reclusão de 1 a 5 anos, além de multa. Este crime tem se tornado cada vez mais comum com o aumento do uso de redes sociais e plataformas de compartilhamento de conteúdo, prejudicando vítimas tanto psicologicamente quanto socialmente.

Pode-se concluir que os crimes contra a honra na *internet* englobam a calúnia, injúria e difamação, tipificados no Código Penal Brasileiro. Contudo, na *internet*, esses

crimes assumem uma nova dimensão devido à rapidez com que as informações se disseminam. As redes sociais, *blogs* e outros meios digitais amplificam o dano causado à imagem da vítima, tornando mais difícil reparar os danos à reputação e à honra. A natureza da *internet* facilita a propagação de mentiras e ofensas de maneira global, ampliando o alcance do impacto negativo.

Vejamos que:

> É certo que, quando alguém pratica determinada infração penal, o Estado sofre, mesmo que indiretamente, com esse tipo de comportamento, devendo, outrossim, punir o infrator para que este não volte a delinquir (efeito preventivo especial da pena), bem como para que os demais cidadãos não o tomem como exemplo (efeito preventivo geral da pena) e venham também a praticar crimes em virtude da sensação de impunidade que gera quando alguém, mesmo tendo transgredido a lei penal editada formalmente pelo Estado, não sofre qualquer reprimenda (Greco, 2018, p. 866).

Assim, ressaltando o grande desafio que a criminalidade digital impõe à investigação e à responsabilização penal. O anonimato proporcionado pela *internet*, somado à dificuldade de rastrear os infratores, cria um cenário complexo para a aplicação da lei, exigindo maior atualização da legislação e melhores ferramentas de investigação para combater eficazmente esses crimes.

ESPÉCIES DE CRIMES E AS DIFICULDADES NO COMBATE À CRIMINALIDADE VIRTUAL

A era digital não trouxe apenas inovação e conectividade, mas também uma gama de novas possibilidades para a prática de atos ilícitos. O advento da *internet* e a proliferação de dispositivos conectados ampliaram exponencialmente as formas e os locais em que os crimes podem ser cometidos.

A velocidade com que as informações circulam na rede facilita a disseminação de práticas criminosas, como fraudes financeiras, roubos de dados e a violação de direitos da personalidade. Essa transformação exige uma reavaliação das ferramentas legais existentes para lidar com esses novos fenômenos. Recentemente estudos indicaram que os crimes cibernéticos estão se tornando mais frequentes, com um aumento significativo no número de incidentes de fraude *online*, invasão de dispositivos e o uso de tecnologias para perpetuar crimes tradicionais. A segurança cibernética, muitas vezes, fica atrás das necessidades urgentes de adaptação legal e técnica para lidar com o crescente volume de ataques. Vejamos o seguinte:

> A internet veio para trazer diversas facilidades na vida das pessoas, sejam para utiliza-la de boa-fé como também de má-fé. Com o aumento significativo do seu uso, surgiram os crimes através dessa plataforma, se fazendo necessário criar legislações que tratassem restritamente desse ambiente e protegessem os usuários que viessem a se tornar vitimas deles, com esse intuito foram criadas algumas legislações de acordo com o aumento desses golpes, bem como para atender as necessidades desse novo tipo penal (Nogueira; Damaceno, 2022, p. 183.)

Os crimes cibernéticos abrangem uma ampla gama de condutas ilícitas, que vão desde fraudes financeiras, como o *phishing* e o roubo de identidade, até crimes contra a honra e a imagem, como a disseminação não autorizada de imagens íntimas. Além disso, é possível observar a ocorrência de crimes de extorsão virtual, como os ataques de *ransomware*, em que criminosos exigem resgates financeiros para liberar dados ou sistemas bloqueados. O uso de redes privadas virtuais (*VPNs*) e o anonimato proporcionado por tecnologias como criptografia contribuem para a complexidade das investigações e dificultam a identificação de criminosos.

Á complexidade para o combate à criminalidade, uma vez que envolvem não apenas barreiras técnicas, mas também entraves legislativos e institucionais. No campo técnico, a constante evolução das tecnologias utilizadas pelos criminosos exige que os sistemas de segurança sejam atualizados regularmente para evitar brechas que possam ser exploradas. É notável a rapidez a qual os golpistas podem evoluir com a chegada de novas tecnológicas, criando sistemas fraudulentos e assim dificultando o combate as atividades criminosas (Menezes, 2016).

No âmbito legislativo, muitos países, incluindo o Brasil, enfrentam a dificuldade de criar leis que acompanhem o ritmo das inovações tecnológicas, o que gera um vácuo jurídico em muitas situações.

Além disso, os entraves institucionais também são um fator significativo, pois nem todos os órgãos responsáveis pela repressão ao crime digital estão adequadamente equipados ou capacitados para lidar com a complexidade dos crimes virtuais. Sem profissionais especializados, bem como a ausência de uma cooperação mais efetiva entre as autoridades nacionais e internacionais, agrava ainda mais o problema.

A combinação dessas barreiras técnicas, legislativas e institucionais cria um ambiente onde os crimes digitais continuam a proliferar, exigindo uma resposta mais integrada e eficiente.

Crimes de Difícil Identificação e Rastreamento

Crimes cibernéticos, pela sua própria natureza, são caracterizados pela fluidez e pelo anonimato, aspectos que dificultam consideravelmente a identificação dos responsáveis. A utilização de tecnologias que mascaram a identidade do criminoso, como as redes privadas virtuais (*VPNs*), as redes *Tor (The Onion Router)* e proxies, complica ainda mais a tarefa das autoridades em rastrear os agentes envolvidos. Tais ferramentas permitem que os infratores ocultem sua localização e alterem sua identidade digital, criando um ambiente no qual é difícil, se não impossível, vincular a atividade criminosa a uma pessoa específica ou a uma jurisdição particular. Vejamos um alerta:

> Um dos principais desafios dos crimes virtuais é a dificuldade de identificar os criminosos e coletar provas, muitos desses crimes são cometidos por pessoas que estão em outro país ou até mesmo em outra região do mundo, alguns criminosos utilizam até de meios mais sofisticados como o uso da VPN (REDE PRIVADA VIRTUAL) que consiste em ser uma técnica que visa ocultar o endereço IP do dispositivo que está sendo utilizado para cometer crimes virtuais, dificultando a identificação do autor das atividades criminosas e, consequentemente, a sua captura pelas autoridades, tornando a investigação e punição dos criminosos um processo complexo e muitas vezes frustrante (Almeida, 2023, p. 8).

O que evidencia a necessidade de abordagens inovadoras para combater essa criminalidade. Logo muitos crimes virtuais são cometidos por intermédio de *bots* ou sistemas automatizados, que operam em grande escala, muitas vezes usando contas falsas ou até mesmo contas roubadas. Isso amplia o anonimato dos infratores e torna ainda mais difícil o processo de rastreamento.

Como a operação desses *bots* ocorre de maneira automatizada e em massa, a obtenção de provas concretas torna-se uma tarefa ainda mais árdua, pois as atividades dos criminosos são dispersas, e as provas frequentemente estão em diversos servidores espalhados pelo mundo. Em muitos casos, é necessário recorrer a técnicas de perícia digital especializadas, que envolvem a análise detalhada de dispositivos, redes e sistemas, além da colaboração de empresas de tecnologia, que, muitas vezes, detêm os registros necessários para identificar os responsáveis.

Por sua vez, a coleta de provas digitais exige rapidez e precisão, visto que as evidências podem ser apagadas, criptografadas ou transferidas rapidamente para servidores localizados fora do país, o que representa um obstáculo adicional. A

volatilidade das provas digitais e a rapidez com que os criminosos se adaptam a novas tecnologias exigem que as investigações sejam conduzidas de maneira ágil e com alta especialização técnica. Como destacou Pereira (2024), "[...] a volatilidade e a possibilidade de alteração das fontes de prova demandam rapidez na captura para preservar os possíveis elementos de prova, especialmente quando se trata de dados em trânsito na rede". Essa dinâmica tem levado a uma maior pressão para que o sistema de justiça seja capaz de lidar com a natureza efêmera e global dos crimes virtuais.

A complexidade das investigações e a necessidade de recursos especializados foram reconhecidas pela jurisprudência brasileira. No caso do Habeas Corpus nº 598.051/SP, o Superior Tribunal de Justiça (STJ) destacou que, dada a natureza transnacional dos crimes virtuais, a obtenção de provas exige “medidas técnicas especializadas e, muitas vezes, a cooperação internacional, dada a natureza transfronteiriça das condutas ilícitas”. Este entendimento do STJ reforça a necessidade de um esforço conjunto entre diferentes países e a utilização de técnicas avançadas para a coleta e validação das provas no contexto digital, sublinhando as limitações enfrentadas pelas autoridades em um cenário de criminalidade virtual cada vez mais globalizado.

Limitações Legislativas

Nossa legislação, embora tenha avançado em algumas áreas, ainda está em um processo de adaptação à realidade digital. Embora a promulgação da Lei nº 12.737/2012, a famosa Lei Carolina Dieckmann, tenha sido um marco importante ao tipificar a invasão de dispositivos eletrônicos e crimes relacionados, e a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados - LGPD) tenha sido um passo significativo no tratamento e proteção dos dados pessoais, muitos crimes ainda não têm uma previsão legal específica.

O princípio da legalidade, previsto na Constituição Federal e no Código Penal, estabelece que ninguém pode ser punido sem uma lei anterior que defina a infração. Esse princípio visa limitar a atuação estatal e proteger a liberdade dos indivíduos, impedindo o exercício de poder arbitrário (Sanches, 2016; Moraes, 2007).

A dinâmica das novas tecnologias e as formas inéditas de criminalidade surgidas no ambiente digital exigem uma constante atualização do ordenamento jurídico, algo que, na prática, ainda não ocorre de forma ágil e eficiente.

Um importante desafio reside no fato de que muitas das leis existentes foram criadas com base em uma realidade analógica, e sua aplicação no contexto digital se torna, muitas vezes, inadequada. Por exemplo, o Código Penal Brasileiro foi modificado pontualmente, mas ainda não contempla adequadamente a complexidade de novos delitos, como os praticados por meio de engenharia social, fraudes envolvendo criptomoedas ou ataques cibernéticos coordenados por inteligência artificial. Esses crimes são mais difíceis de tipificar e muitas vezes escapam à regulação de normas tradicionais, tornando-se um desafio para os operadores do Direito. Além disso, a velocidade com que surgem novas modalidades de crimes virtuais torna a legislação ainda mais defasada.

De acordo com Dias (2007), a regularização das práticas realizadas no ambiente virtual é uma questão urgente, especialmente no que diz respeito às situações que não estão em conformidade com a legislação vigente, tendo em vista seus impactos no sistema jurídico. A autora ressalta que um ordenamento jurídico fundamentado na previsibilidade é essencial para garantir a segurança jurídica dos cidadãos.

A deficiência de normas penais claras e específicas no campo dos crimes digitais gera uma série de problemas práticos. Primeiramente, ela contribui para uma insegurança jurídica, o que prejudica a atuação de magistrados e promotores, que muitas vezes se veem diante de situações novas sem uma orientação normativa precisa. A inexistência de uma tipificação clara para diversos tipos de crimes digitais faz com que o Direito precise recorrer a analogias ou interpretações extensivas, o que pode gerar decisões jurídicas contraditórias ou insatisfatórias. Isso, por sua vez, contribui para a impunidade de infratores e a sensação de fragilidade do sistema de justiça.

Um outro ponto crítico que deve ser considerado é a divergência interpretativa, que se reflete, por exemplo, nas discussões sobre a tipificação de crimes relacionados à liberdade de expressão nas redes sociais. O discurso de ódio, as *fakes news* e outros crimes de opinião geram debates acalorados sobre quais limites devem ser impostos à liberdade de expressão no ambiente digital.

De acordo com um estudo sobre discursos de ódio em redes sociais, esses discursos geralmente se caracterizam por incitar a discriminação contra indivíduos que compartilham uma característica identitária comum, como cor da pele, gênero, orientação sexual, nacionalidade, religião, entre outros atributos (Universidade Federal de Santa Maria, 2025).

A ausência de uma regulamentação específica para essas questões levanta dilemas sobre os direitos individuais e a necessidade de garantir a ordem pública no ambiente virtual. Esse vácuo legal não apenas facilita a impunidade, mas também intensifica a sensação de insegurança e desconfiança na *internet*, que se torna um espaço em que as ações criminosas, por vezes, permanecem impunes ou com poucas consequências jurídicas.

Diante desse panorama, a legislação brasileira precisa urgentemente evoluir e se adaptar às novas realidades digitais, promovendo uma regulação mais precisa, eficaz e equilibrada, que consiga não apenas garantir a proteção dos cidadãos, mas também não inibir o desenvolvimento tecnológico e a liberdade de expressão no ambiente virtual.

Cooperação Internacional e Jurisdição

A *internet* permitindo a comunicação e a realização de atividades sem limitações geográficas, cria um ambiente propício para a ocorrência de crimes cibernéticos de caráter transnacional. A ausência de fronteiras físicas no ciberespaço facilita a atuação de criminosos em locais distantes, o que gera desafios significativos para a repressão e a responsabilização penal. Crimes como fraudes financeiras, lavagem de dinheiro, tráfico de drogas e pornografia infantil, muitas vezes, são perpetrados por indivíduos localizados em países que não mantêm acordos de cooperação internacional com o Brasil ou que adotam legislações mais permissivas, que tornam a repressão à criminalidade digital ainda mais difícil.

Podemos estacar que, apesar de a *internet* permitir a transgressão de barreiras físicas, as limitações jurídicas e diplomáticas impõem obstáculos substanciais à repressão de crimes cibernéticos.

Segundo Quaglio (2021), é evidente a relevância de se estudar o fenômeno das fake news sob a perspectiva do direito internacional, considerando os meios de cooperação jurídica já existentes. A autora defende que se priorize o uso dessas

ferramentas em vez de propor inovações legislativas apressadas e desprovidas de um debate mais amplo e aprofundado.

A localização de servidores em países fora da jurisdição nacional, por exemplo, dificulta a coleta de provas essenciais para a instrução processual. Em alguns casos, esses servidores estão em países com legislações mais brandas ou inexistentes sobre crimes digitais, o que complica ainda mais a obtenção de dados ou a responsabilização dos autores.

Sem uma regulamentação uniforme e de uma rede de cooperação sólida entre as nações representa uma lacuna crítica no combate à criminalidade cibernética. Embora o Brasil seja signatário de acordos bilaterais e participe de iniciativas internacionais, como a Convenção de Budapeste sobre o Cibercrime, ainda há uma considerável dificuldade na implementação efetiva desses tratados, principalmente no que tange à troca de informações e à execução de medidas punitivas. A Convenção de Budapeste estabelece princípios e obrigações para a cooperação internacional, muitos países possuem diferentes graus de rigor na aplicação de suas normas sobre crimes digitais.

Conforme aponta Quaglio (2021), o Brasil enfrenta dificuldades para obter dados de usuários em investigações sobre crimes cibernéticos, como os relacionados às fake news, pois muitas vezes as autoridades recorrem diretamente às subsidiárias das empresas, que não detêm os dados. A autora observa que essa prática ignora os procedimentos legais previstos tanto no direito brasileiro quanto no direito internacional, que exigem o uso da cooperação judicial internacional para acessar informações controladas fora do país.

Essa situação se agrava em crimes como pornografia infantil, lavagem de dinheiro via criptomoedas e crimes contra sistemas financeiros, onde as transações digitais podem ser mascaradas e deslocadas para jurisdições mais flexíveis, criando um cenário em que os criminosos conseguem operar com relativa impunidade.

A falta de uma padronização internacional nas normas de privacidade, proteção de dados e regras de investigação gera dificuldades na obtenção de provas, com diferentes países adotando diferentes níveis de vigilância e regulamentação. Logo, é evidente que o combate à criminalidade digital exige não apenas a adaptação da legislação interna, mas também uma atuação mais integrada e eficiente no âmbito internacional.

O fortalecimento de tratados multilaterais, a harmonização das normas e a intensificação da cooperação entre os países são fundamentais para garantir que as vítimas da criminalidade digital tenham acesso à justiça, independentemente das fronteiras nacionais.

Capacitação Técnica dos Agentes Públicos

A criminalidade digital exige que os profissionais do sistema de justiça criminal estejam devidamente preparados para lidar com os complexos aspectos técnicos das investigações. A constante evolução da tecnologia, que gera novas formas de delitos virtuais, exige uma atualização contínua de conhecimentos e especialização em áreas como cibersegurança, análise de *logs*, engenharia reversa, criptografia, entre outras. Porém, a realidade é que o sistema de justiça no Brasil ainda enfrenta dificuldades significativas em termos de capacitação e preparo técnico adequado para lidar com esses crimes.

Segundo os dados do Ministério da Justiça (2022), apenas 18% das delegacias no Brasil possuem núcleos especializados em crimes digitais, e, ainda mais preocupante, "menos de 20% dos delegados possuem formação técnica específica para atuar em investigações virtuais". Esse déficit no treinamento específico compromete a eficiência das investigações e aumenta o risco de falhas no processo, dificultando a coleta de provas e a resolução dos casos. A falta de conhecimento especializado também pode gerar insegurança jurídica, pois provas digitais podem ser desconsideradas ou mal interpretadas, prejudicando a efetividade do processo judicial.

A eficácia do combate à criminalidade digital depende diretamente da capacitação técnica dos profissionais envolvidos:

> A aplicação eficaz da legislação é essencial para proteger a sociedade. As autoridades deverão dispor de recursos e capacidade técnica para investigar e rastrear os ataques cibernéticos. Isso inclui o uso de tecnologia avançada e a colaboração com especialistas em segurança cibernética. Além disso, é importante que as leis sejam aplicadas de maneira consistente, independentemente da localização do infrator (Maia e Costa, 2023, p. 123).

Sem o devido treinamento, os investigadores podem ter dificuldades em manusear as ferramentas necessárias para coletar evidências, como *logs* de

servidores, rastreamento de endereços *IP* ou a análise de sistemas criptografados, prejudicando a investigação.

Além dos profissionais da polícia, é essencial que membros do Judiciário e do Ministério Público possuam conhecimentos básicos sobre o funcionamento da *internet* e das tecnologias envolvidas nos crimes digitais. A falta de preparo técnico pode resultar na desconsideração de provas digitais, ineficácia nas diligências realizadas e até mesmo no arquivamento indevido de inquéritos.

Logo, a capacitação dos profissionais envolvidos no combate à criminalidade digital não é apenas uma questão de atualização de conhecimentos, mas uma necessidade fundamental para o fortalecimento do sistema de justiça. É necessário que haja investimentos contínuos em treinamentos especializados e em tecnologias de ponta, a fim de que as investigações possam ser conduzidas de maneira eficaz e as provas digitais possam ser corretamente analisadas e utilizadas no processo judicial.

CONSIDERAÇÕES FINAIS

A análise desenvolvida neste trabalho revelou que o enfrentamento da criminalidade digital exige uma abordagem complexa e multifacetada, indo além da simples aplicação de normas jurídicas existentes. A constante evolução tecnológica impõe ao Direito o desafio de se atualizar para lidar com novas modalidades de delitos virtuais, compreendendo suas dinâmicas, os atores envolvidos e desenvolvendo estratégias eficazes de repressão e prevenção.

Um dos principais obstáculos enfrentados é a dificuldade de identificar e rastrear criminosos, devido ao uso de tecnologias como anonimato, criptografia e redes descentralizadas. Esses recursos dificultam as investigações e exigem ferramentas técnicas muitas vezes indisponíveis às autoridades. Além disso, a legislação vigente ainda apresenta lacunas, mesmo com avanços como a Lei nº 12.737/2012 (Lei Carolina Dieckmann) e a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), sendo necessária a tipificação de novas condutas e a harmonização entre legislações nacionais e internacionais.

A cooperação internacional é fundamental, pois muitos crimes ultrapassam fronteiras e envolvem múltiplas jurisdições. A atuação conjunta entre países, por meio de tratados e redes de comunicação, é essencial para investigações e responsabilizações eficazes. Também é urgente a capacitação técnica de agentes

públicos. Conhecimentos em segurança da informação, análise forense digital, investigação cibernética e legislação especializada são indispensáveis para o desempenho eficiente de suas funções.

Conclui-se que o combate à criminalidade digital demanda investimentos contínuos em tecnologia, atualização legislativa, cooperação institucional e capacitação profissional, além da promoção da educação digital da população para garantir segurança jurídica e proteção de direitos no ambiente virtual.

REFERÊNCIAS

ALMEIDA, Ruanh Neres de. **Estelionato virtual no direito brasileiro**. 2023. Trabalho de Conclusão de Curso (Graduação em Direito) – Pontifícia Universidade Católica de Goiás, Escola de Direito, Negócios e Comunicação, Goiânia, 2023. Disponível em: https://repositorio.pucgoias.edu.br/jspui/handle/123456789/6205. Acesso em: 23 abr. 2025.

ALMEIDA, Jessica de Jesus; MENDONÇA, Allana Barbosa; DO CARMO, Gilmar Passos; SANTOS, Kendisson Souza; SILVA, Luana Munique Meneses; DE AZEVEDO, Roberta Rayanne Dória. Crimes cibernéticos. **Caderno de Graduação - Ciências Humanas e Sociais** - UNIT - SERGIPE, *[S. l.]*, v. 2, n. 3, p. 215–236, 2015. Disponível em: https://periodicos.grupotiradentes.com/cadernohumanas/article/view/2013. Acesso em: 7 maio. 2025.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos. **Diário Oficial da União**, Brasília, DF, 2012.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**, Brasília, DF, 2018.

BRASIL. **Ciências Policiais.** Brasília, v. 4, n. 1, p. 61–85, jan./jun. 2013. Disponível em: https://www.revistacienciaspoliciais.org/a-descoberta-e-a-analise-de-vinculos-na-complexidade-da-investigacao-criminal-moderna/. Acesso em: 7 maio 2025.

DIAS, Virgínia Soprana. **Aspectos da segurança jurídica no âmbito dos crimes cibernéticos.** ICoFCS, 2007. Disponível em: http://www.icofcs.org/2007/ICoFCS2007-pp12.pdf. Acesso em: 7 maio 2025.

FERRO JÚNIOR, Celso Moreira; LIMA, George Felipe de. A descoberta e a análise de vínculos na complexidade da investigação criminal moderna. 2013. Disponível: https://www.conteudojuridico.com.br/consulta/artigos/14759/a-descoberta-e-a-analise-de-vinculos-na-complexidade-da-investigacao-criminal-moderna. Acesso em: 13-jan-2025.

FIORILLO, Celso Antonio Pacheco; CONTE, Christiany Pegorari. **Crimes no Meio Ambiente Digital.** 2. ed. São Paulo: Saraiva, 2016.

GRECO, Rogério. **Curso de direito penal:** parte geral, volume I.19. ed. Niterói: Impetus, 2018.

MAIA, Karolline Barbosa; COSTA, Cezar Henrique Ferreira. CRIMES CIBERNÉTICOS . Revista Ibero-Americana de Humanidades, Ciências e Educação, *[S. l.]*, v. 9, n. 10, p. 109–126, 2023. DOI: 10.51891/rease.v9i10.11580. Disponível em: https://periodicorease.pro.br/rease/article/view/11580. Acesso em: 23 abr. 2025.

MATSUYAMA, Keniche Guimarães; LIMA, João Ademar de Andrade. *Crimes cibernéticos: atipicidade dos delitos*. Caderno de Graduação – Ciências Humanas e Sociais – UNIT – Sergipe, [S. l.], v. 2, n. 3, p. 237–250, 2015. Disponível em: https://periodicos.grupotiradentes.com/cadernohumanas/article/view/2013/1217. Acesso em: 7 maio 2025.

MENEZES, Elsio Gomes de Araujo. A prescrição no crime de estelionato previdenciário. Edunit, abril 2016. Disponível em: https://periodicos.set.edu.br/ideiaseinovacao/article/view/2993/1596. Acesso em: 19 abr. 2025.

MINISTÉRIO DA JUSTIÇA. *Relatório sobre o Combate à Criminalidade Digital no Brasil*. Brasília: MJ, 2022.

MORAES, Alexandre de. **Direitos Humanos Fundamentais:** Teoria geral, comentários aos arts. 1º a 5º da Constituição da República Federativa do Brasil, doutrina e jurisprudência. 8ª Ed. São Paulo: Saraiva, 2007.

NOGUEIRA, Isabella de Melo Ramalho; DAMASCENO, Lívia Ximenes. **Produção técnica:** descomplicando o Direito Civil. In: BRAGA, Daniel L. S. (Org.). 2022. Disponível: https://institutoscientia.com/wp-content/uploads/2022/10/Livro-Direito-2.pdf. Acesso em: 15-fev-2025.

PEREIRA, Beatriz Alves. **As provas digitais no processo penal: uma análise de seus atributos e seus standards metodológicos**. 2024. 74 f. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Faculdade Nacional de Direito, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2024. Disponível em: http://hdl.handle.net/11422/24251. Acesso em: 23 abr. 2025.

QUAGLIO, Laura Oliveira. **Jurisdição internacional e as fake news na era da pós-verdade: uma análise das leis no âmbito do direito digital vigentes no Brasil e o PL nº 2630/2020.** 2021. 26 f. Trabalho de Conclusão de Curso (Graduação em Direito) – Universidade Federal de Uberlândia, Uberlândia, 2021. Disponível em: https://repositorio.ufu.br/handle/123456789/32132. Acesso em: 7 maio 2025.

SANTANA SILVA, Diego Leonardo. Seriam as máquinas capazes de sonhar? Uma introdução à história da internet. **Boletim Historiar,** *[S. l.]*, n. 15, 2016. Disponível em: https://periodicos.ufs.br/historiar/article/view/5584. Acesso em: 17 abr. 2025.

TOFFOLO HOFFELDER, J.; CASTRO, M. F. de. ESTELIONATO ELETRÔNICO: Necessidade de Tipificação Legal? **Anuário Pesquisa e Extensão Unoesc São Miguel do Oeste**, *[S. l.]*, v. 3, p. e19789, 2018. Disponível em: https://periodicos.unoesc.edu.br/apeusmo/article/view/19789. Acesso em: 7 maio. 2025.

UNIVERSIDADE FEDERAL DE SANTA MARIA**. Discursos de ódio em redes sociais: jurisprudência brasileira.** Dez. 2011. Disponível em: https://www.scielo.br/j/rdgv/a/QTnjBBhqY3r9m3Q4SqRnRwM/. Acesso em: 7 maio 2025.