B1 ISSN: 2595-1661

ARTIGO ORIGINAL

Listas de conteúdos disponíveis em Portal de Periódicos CAPES

Revista JRG de Estudos Acadêmicos

Página da revista:
https://revistajrg.com/index.php/jrg

ISSN: 2595-1661
Revista JRG de Estudos Acadêmicos

CRIMES CIBERNÉTICOS: desafios jurídicos no processo e julgamento de infrações penais virtuais cometidas por agentes estrangeiros contra vítimas brasileiras

CYBER CRIMES: legal challenges in the process and judgment of virtual criminal offenses committed by foreign agents against Brazilian victims

DOI: 10.55892/jrg.v7i15.1563
ARK: 57118/JRG.v7i15.1563

Recebido: 09/11/2024 | Aceito: 15/11/2024 | Publicado *on-line*: 16/11/2024

Julio Cesar Lôbo da Costa Gomes[1]
https://orcid.org/0009-0005-0471-5016
https://lattes.cnpq.br/1519650885523561
Faculdade de Ciências Jurídicas de Paraíso do Tocantins, TO, Brasil
E-mail: juliocesargomes21498@gmail.com

Lucas Cavalcante Medrado[2]
https://orcid.org/0009-0000-7610-5085
http://lattes.cnpq.br/3159312206142733
Faculdade de Ciências Jurídicas de Paraíso do Tocantins, TO, Brasil
E-mail: lucas.cavalcante2018@gmail.com

Giliarde Benavinuto Albuquerque Cavalcante Virgulino Ribeiro Nascimento e Gama[3]
https://orcid.org/0000-0001-8146-6811
http://lattes.cnpq.br/4525837393612907
Faculdade de Ciências Jurídicas de Paraíso do Tocantins, TO, Brasil
E-mail: benavinutogama@gmail.com

Resumo

Os crimes cibernéticos representam um desafio crescente para os sistemas jurídicos nacionais e internacionais, especialmente quando envolvem agentes estrangeiros e vítimas localizadas em outras jurisdições, como o Brasil. A globalização digital permite que infratores cibernéticos atuem a partir de qualquer lugar do mundo, utilizando redes virtuais para praticar fraudes, extorsões, vazamento de dados, entre outras infrações, atingindo diretamente cidadãos e organizações de outros países. No contexto brasileiro, quando o crime for cometido por um agente estrangeiro, surgem barreiras jurídicas relacionadas à jurisdição, cooperação internacional, e à aplicação da legislação nacional em casos que envolvem múltiplas soberanias. O processo de investigação e julgamento dessas infrações exige articulação entre diversas instituições internacionais, como tratados de cooperação e acordos bilaterais, além da adaptação de normas que regem o direito penal para o ambiente virtual. O presente

[1] Graduando em Direito pela Faculdade de Ciências Jurídicas de Paraíso do Tocantins.
[2] Advogado. Especialista em Direito Penal, Processo Penal e Prática Judiciária. Docente do curso de Direito da Faculdade de Ciências Jurídicas de Paraíso do Tocantins (FCJP).
[3] Doutorando (PPGDR/UFT). Mestre (PPGDCOMS/UFT). Especialista em Direito e Processo Tributário, em Direito e Processo Penal, em Criminologia, em Direito e Processo do Trabalho. Graduado em Direito (UFT). Professor da Faculdade de Ciências Jurídicas de Paraíso do Tocantins (FCJP), na Escola Superior de Gestão Penitenciária e Prisional do Tocantins, na pós-graduação na Universidade Estadual do Tocantins. Coordenador Jurídico e Correcional do Sistema Penal do Tocantins (SECIJU/TO)

estudo tem como objetivo verificar os procedimentos aplicáveis aos casos de crimes cibernéticos cometidos por agentes estrangeiros contra vítimas brasileiras, analisando as barreiras e as soluções jurídicas. Para tanto, utilizou-se a metodologia da pesquisa jurídica e o método teórico dedutivo, recorrendo à pesquisa exploratória bibliográfica e documental, pautada em legislações vigentes, produções científicas e acervos doutrinários sobre o tema. Conclui-se que a cooperação internacional e o aprimoramento da legislação nacional são cruciais para o enfrentamento das infrações penais praticadas no ambiente virtual. Assim, o presente estudo contribui para a reflexão sobre as necessidades de avanços legislativos e institucionais para o combate aos crimes cibernéticos, reforçando a importância de um sistema jurídico adaptado à realidade digital global.

Palavras-chave: Crimes cibernéticos; Agentes estrangeiros; Cooperação internacional; Jurisdição; Legislação brasileira.

Abstract
Cybercrimes represent a growing challenge for national and international legal systems, especially when they involve foreign agents and victims located in other jurisdictions, such as Brazil. Digital globalization allows cyber criminals to act from anywhere in the world, using virtual networks to commit fraud, extortion, data leaks, among other infractions, directly affecting citizens and organizations from other countries. In the Brazilian context, when the crime is committed by a foreign agent, legal barriers arise related to jurisdiction, international cooperation, and the application of national legislation in cases involving multiple sovereignties. The process of investigating and judging these infractions requires coordination between several international institutions, such as cooperation treaties and bilateral agreements, in addition to the adaptation of rules that govern criminal law for the virtual environment. The present study aims to verify the procedures applicable to cases of cybercrime committed by foreign agents against Brazilian victims, analyzing the barriers and legal solutions available. The methodology used is a bibliographical review, based on legal and doctrinal materials on the topic. It is concluded that international cooperation and the improvement of national legislation are crucial to face these challenges effectively, thus the continuous improvement of national legislation is essential for the protection of Brazilian citizens and organizations, preventing and punishing, more efficiently, such as infractions committed in a virtual environment. In this way, this study contributes to the reflection on the legislative and institutional needs to combat cybercrimes, reinforcing the importance of a legal system adapted to the global digital reality.

Keywords: Cybercrimes; Foreign Agents; International Cooperation; Jurisdiction; Brazilian Legislation.

1. Introdução

Com o advento da tecnologia, ocorreu a aceleração do desenvolvimento e o rompimento de fronteiras, ao passo que isso possibilitou a humanidade alcançar grandes avanços nos mais diversos aspectos. No entanto, tais avanços vieram acompanhados de certas lacunas a serem observadas sob o viés jurídico e que serão explorados na presente pesquisa.

Nesse contexto de avanço da tecnologia e globalização da internet, os crimes cibernéticos tornaram-se uma preocupação central para as jurisdições de todos os países, incluindo o Brasil. A internet proporciona aos criminosos uma plataforma anônima e de alcance global, permitindo que infratores, independentemente de sua localização, cometam crimes contra indivíduos e instituições em outros países, sem necessidade de presença física.

Nesse cenário, a sofisticação das infrações virtuais, como fraudes, roubos de identidade, ataques de ransomware e disseminação de vírus, coloca em evidência a fragilidade das fronteiras territoriais, uma vez que os criminosos podem estar em qualquer parte do mundo enquanto as vítimas se encontram em outra jurisdição. Essa dinâmica complexa acarreta desafios significativos para o sistema jurídico brasileiro no que tange à investigação, processo e julgamento de crimes que envolvem agentes estrangeiros.

Diante desse cenário, é evidente que o combate aos crimes cibernéticos cometidos por agentes estrangeiros contra vítimas brasileiras exige um esforço coordenado não só do sistema jurídico brasileiro, mas também da comunidade internacional.

O reforço da cooperação entre países, a criação de tratados específicos para a cibercriminalidade e o desenvolvimento de tecnologias avançadas para a investigação de crimes virtuais são apenas alguns dos passos que devem ser tomados para que esses desafios possam ser enfrentados de forma mais eficaz. A integração de normas jurídicas globais e o fortalecimento das capacidades nacionais são elementos cruciais para garantir que a justiça seja alcançada, independentemente das fronteiras virtuais.

Em vista disso, a pesquisa discutirá a seguinte problemática: a atuação do sistema jurídico brasileiro é eficaz nos casos de crimes cibernéticos cometidos por agentes estrangeiros contra vítimas brasileiras, considerando os desafios de jurisdição, cooperação internacional e aplicação da legislação?

O estudo se justifica pela crescente relevância dos crimes cibernéticos no cenário contemporâneo, sobretudo aquelas condutas criminosas que, outrora praticadas de maneira física, agora são praticados virtualmente, razão pela qual dificulta o processo investigativo e punitivo. Sendo assim, o avanço das tecnologias digitais e a globalização da internet tornaram mais fácil para os infratores em diferentes partes do mundo cometerem infrações virtuais contra indivíduos e instituições de outros países. Nesse viés, o Brasil tem enfrentado uma série de desafios, tanto em termos de aplicação de sua legislação penal quanto na promoção de uma cooperação internacional eficiente que permita a investigação e punição desses crimes.

O objetivo geral deste estudo é verificar a incidência da legislação penal em situações que envolvam crimes cibernéticos transfronteiriços, buscando compreender os desafios para seu enfrentamento pelo direito pátrio. Em relação aos objetivos específicos, destacam-se os seguintes: a) conceituar os crimes cibernéticos, oferecendo uma compreensão do que configura ambiente virtual; b) analisar os contornos jurídicos da Lei nº 12.737/2012, conhecida como “Lei Carolina Dieckmann”,

e avaliar sua aplicabilidade no contexto de crimes cibernéticos; c) identificar as barreiras legislativas que podem surgir durante o processo e julgamento de crimes virtuais, apontando possíveis lacunas e limitações que dificultam a punição dos infratores; e d) examinar os mecanismos de cooperação internacional entre o Brasil e outros países na investigação e punição desses crimes.

2. Metodologia

Para tanto, será utilizada a metodologia da pesquisa jurídica e o método teórico dedutivo, recorrendo à pesquisa exploratória bibliográfica e documental, pautada em legislações vigentes, em doutrinas de direito penal, processual penal e digital, além de produções científicas, com abordagem qualitativa.

3. JURISDIÇÃO PENAL E OS CRIMES CIBERNÉTICOS

A jurisdição penal aplicada aos crimes cibernéticos é um campo desafiador e em constante evolução, uma vez que os crimes praticados no ambiente digital rompem as fronteiras geográficas e desafiam os limites das legislações nacionais. Assim conforme Albuquerque e Tiburcio (2023), discorrem sobre os problemas jurisdicionais apresentando duas características da internet que são a raiz do problema:

> duas características da internet estão na origem do problema e têm merecido especial atenção: sua ubiquidade e sua virtualidade. O termo ubiquidade é normalmente utilizado para fazer referência ao fato de que o conteúdo disponível na internet é acessível de forma imediata e simultânea em qualquer parte do planeta, enquanto o termo virtualidade designa a desconexão entre o conteúdo produzido e elementos físicos ou geográficos que permitam sua localização. (ALBUQUERQUE; TIBURCIO, 2023, p. 10).

De acordo com Tocantins (2024), o avanço da tecnologia e o aumento das atividades ilícitas online, que variam desde fraudes e invasões de privacidade até ataques cibernéticos de grande escala e exploração sexual, a necessidade de uma abordagem penal específica e adaptável e se torna crucial.

Portanto, os sistemas jurídicos de diversos países buscam formas de ampliar sua jurisdição para enfrentar crimes cibernéticos, utilizando-se de novas normas territoriais e tratados internacionais que facilitem a cooperação entre autoridades.

Conforme Maria Eduarda Vieira (2023) aborda trazendo em sua análise que a natureza anônima dos crimes digitais e a dificuldade de adaptar conceitos tradicionais do direito penal, como autoria e materialidade, para o ambiente virtual, criam desafios adicionais. A harmonização legislativa e a cooperação internacional, exemplificadas pela Convenção de Budapeste, são essenciais para tornar a jurisdição penal mais eficaz contra as novas formas de criminalidade digital, promovendo a segurança e privacidade em um mundo conectado.

3.1 JURISDIÇÃO E TERRITORIALIDADE

De acordo com Sanches (2019, p. 31) “a lei penal de um país está diretamente ligada à sua soberania, daí porque sua validade aparece limitada no espaço dentro do qual se reconhece, na comunidade internacional, o exercício dessa soberania.” Ressalta o autor que a prática de uma infração penal pode desenvolver em lugares diversos, transitando o território de mais de um país com igualdade de soberanias, ocasionando aparente conflito internacional de jurisdição.

Nesse contexto, a jurisdição penal aplicada aos crimes cibernéticos enfrenta desafios complexos e crescentes à medida que o ambiente digital se torna uma parte

fundamental da vida cotidiana e, consequentemente, do cenário criminal. Marra (2019) aponta que o conceito de jurisdição e territorialidade é primordial para o direito, pois estabelece os limites de atuação dos Estados na repressão a crimes.

Segundo Alves (2024, p. 349) "a jurisdição é o poder soberano do Estado de dizer o direito no caso concreto, resolvendo conflitos, em substituição à vontade das partes. A substitutividade é, pois, a característica mais marcante desse poder." Capez (2013, p. 58) descreve que "a jurisdição é, portanto, a função, o processo, o instrumento de sua atuação. Sem processo não há como solucionar o litígio, razão por que é instrumento imprescindível para resguardo da paz social."

Os limites desse território devem ser reconhecidos não apenas por seus compatriotas, mas externamente, "[...] ou seja, pelos demais Estados-nações, num reconhecimento mútuo de seus espaços jurisdicionais." (ISRAEL, 2020, p. 72). Contudo, quando se trata de crimes cibernéticos, a definição tradicional de jurisdição baseada em fronteiras geográficas é posta sob discussão. Essas características tornam difícil a aplicação de normas tradicionais de territorialidade, desafiando, assim, os sistemas jurídicos a compensar seus critérios de jurisdição para dar uma resposta eficaz ao cibercrime.

Nesse cenário, Israel (2020, p. 74) explica que:

> O território se define sobretudo pelo processo de apropriação espacial e pelo poder que nele se exerce, independentemente de sua forma, zonal ou em rede, e dos sujeitos que protagonizam a ação, quer sejam esses o Estado, as empresas ou a sociedade civil. Essa concepção de território nos permite reler o exercício da atividade política e jurisdicional em tempos de globalização e, principalmente, compreender o ciberespaço a partir da lógica socioespacial de sua base, a Internet.

Milagre (2021), ao discutir a Lei de Crimes Informáticos (Lei 14.155/2021), enfatiza que, no contexto digital, uma invasão de dispositivos informáticos é um dos crimes que mais exige uma nova abordagem jurisdicional. Esse tipo de delito levanta questões técnicas e controversas, especialmente no que diz respeito à caracterização da "invasão", que pode ocorrer em múltiplas jurisdições ao mesmo tempo. A extraterritorialidade desse tipo de crime desafia as fronteiras do direito penal clássico, uma vez que é difícil definir onde o crime efetivamente se inicia e onde ele causa impacto.

Milagre (2021) argumenta que a lei brasileira tentou definir parâmetros mais claros para a invasão de dispositivos informáticos, mas ainda resta incertezas quanto à eficácia da aplicação e à cooperação internacional para a proteção de infratores.

Salienta Edinilson Santos Vieira ([2023]) corroborando com essa perspectiva ao discutir as características dos crimes cibernéticos como um problema global, que exige esforços internacionais de cooperação e adaptação das legislações nacionais. Segundo o autor, os países devem harmonizar seus sistemas legais e processos judiciais para permitir uma resposta ágil e eficaz aos crimes cometidos online. Ele também destaca que, na prática, muitos dos cibercriminosos utilizam ferramentas e métodos para mascarar sua localização, dificultando a aplicação das leis de um país específico e a cooperação entre as autoridades.

Para Jêior (2019), o conceito de jurisdição na internet deve ser abordado de forma mais ampla e flexível, adaptando-se ao caráter fluido do ciberespaço. Ele propõe uma expansão do conceito de territorialidade para incluir a ideia de "território virtual", no qual as normas podem ser aplicadas não apenas com base no local físico, mas também no espaço digital onde o crime ocorre. Essa abordagem inovadora pode

estabelecer uma base legal para que as autoridades atuem em casos onde, embora não exista um território físico específico, o impacto das ações cibernéticas afete direta e significativamente o território nacional. Jêior (2019) observa que essa redefinição de território é crucial para que o direito penal não perca sua eficácia frente à evolução tecnológica.

Nesse viés, Marra (2019) destaca sobre a necessidade de os Estados adaptarem suas leis para refletir o impacto do crime cibernético e tratarem questões como a territorialidade de forma mais colaborativa. Ela aponta que os crimes cibernéticos exigem uma ação coordenada entre os países, uma vez que as atividades ilícitas online não respeitam fronteiras. Todavia, as diferenças culturais e legais entre os países criam obstáculos para a criação de normas internacionais harmonizadas. Marra sugere que uma solução seria o fortalecimento dos tratados multilaterais como a Convenção de Budapeste, que visa criar um padrão mínimo de legislações contra o crime cibernético, mas que ainda cuida da adesão global para ser plenamente eficaz.

Milagre (2021) complementa essa visão ao indicar que, além dos tratados, é necessária uma infraestrutura tecnológica adequada para combater os crimes cibernéticos de forma coordenada. Ele argumenta que as autoridades precisam estar equipadas com ferramentas de rastreamento e análise de dados que sejam específicas na identificação da origem dos crimes virtuais e dos agentes envolvidos. Contudo, ele registra que isso levanta questões de privacidade e proteção de dados, uma vez que a coleta de informações digitais é um processo intrusivo que, se mal transitado, pode violar os direitos dos cidadãos. Assim, o autor propõe um equilíbrio entre a necessidade de vigilância e o respeito à privacidade individual, essencial para uma jurisdição penal justa e equilibrada no ambiente digital.

Desse modo, Edinilson Santos Vieira (2023) propõe que o conceito próprio de crime precisa ser revisitado no contexto da internet, onde ações antes consideradas inofensivas podem causar danos em escala global. Ele exemplifica essa ideia com os ataques de negação de serviço (DDoS), que, embora não destruam sistemas fisicamente, podem paralisar empresas e governos. Ainda, salienta que o conceito de territorialidade deve, portanto, incluir tanto o espaço físico quanto o impacto virtual, registrando que os danos na esfera digital têm consequências no mundo real e devem ser tratados com a mesma seriedade.

Por fim, Jêior (2019) ressalta a importância da educação e da conscientização como medidas preventivas contra o crime cibernético, argumentando que as leis, por si só, são insuficientes para lidar com o problema. Ele sugere que é essencial educar a população e os profissionais da área de segurança digital sobre os riscos e responsabilidades do ambiente online, criando uma cultura de prevenção e cuidado no uso das tecnologias. Portanto, a jurisdição penal é apenas uma das ferramentas no combate ao cibercrime, mas uma abordagem multidisciplinar, que envolve educação, tecnologia e cooperação internacional, é crucial para enfrentar de maneira eficaz os desafios do ciberespaço.

3.2 INTERNET E OS CRIMES CIBERNÉTICOS

Conforme Tiburcio e Albuquerque (2023, p. 43) “enquanto a geografia política da modernidade divide o mundo em Estados nacionais separados por fronteiras físicas (rios e montanhas, mares e oceanos, etc), o mundo virtual é dividido por telas e senhas.” Por conseguinte, é notório que a internet tem modificado substancialmente o mundo, não sendo diferente com o cenário criminal, razão por que amplia as possibilidades de atuação e o alcance dos crimes cibernéticos. Para Gomes e Medrado (2023, p. 04) “essa conduta é perpetrada por indivíduos ou entidades

jurídicas, envolvendo a utilização da informática, seja online ou offline, e resulta em uma violação direta ou indireta da segurança cibernética."

Milagre (2021) aponta que, com o advento da Lei nº 14.155/2021, o Brasil deu um passo importante para enfrentar os delitos informáticos, especialmente no que diz respeito à invasão de dispositivos, ainda que existam pontos controversos na aplicação dessa legislação. Em um contexto em que hackers e crimes virtuais aproveitam brechas de segurança para cometer infrações, o autor destaca que a falta de clareza nos critérios para caracterizar uma "invasão" é um desafio específico. As investigações técnicas dos crimes cibernéticos, como o uso de redes complexas e de métodos avançados para ocultar a identidade, tornam a aplicação de leis mais complexas e impedem um esforço contínuo dos legisladores e das autoridades para garantir que as violações sejam identificadas e responsabilizadas.

Corrêa e Monteiro Neto (2023) enfatizam que a adesão do Brasil à Convenção de Budapeste representa um marco na luta contra o cibercrime, pois possibilita uma cooperação internacional sem precedentes. A Convenção, considerada o primeiro tratado internacional sobre crimes cometidos via internet, visa padronizar e fortalecer o combate ao cibercrime em escala global. No entanto, os autores salientam que essa adesão também traz desafios para o Direito Penal, como a necessidade de equilibrar a expansão das normas penais com a proteção dos direitos fundamentais dos indivíduos. A cooperação internacional promovida pela Convenção permite que os países compartilhem informações e coordenem operações, mas é preciso uma regulamentação cuidadosa que possa proporcionar harmonização legislativa e proteção de dados.

Nesse sentido, Silva (2021) aponta a relevância da Convenção de Budapeste como ferramenta essencial na repressão ao crime cibernético no Brasil, argumentando que, sem a cooperação internacional, seria quase impossível investigar e punir eficazmente esses crimes. A natureza transnacional da internet permite que um crime de violação em um país tenha consequências em várias partes do mundo, tornando a atuação conjunta entre nações necessárias. O autor ainda propõe que, embora o Brasil tenha se beneficiado da cooperação jurídica internacional fornecida pela Convenção, ainda há dificuldades práticas, como a falta de recursos tecnológicos adequados e a necessidade de treinamento especializado das autoridades locais para acompanhar a sofisticação crescente dos ataques virtuais.

Name (2023) discute os impactos dos crimes cibernéticos na imagem e privacidade dos indivíduos, um aspecto particularmente especial no ambiente digital. Segundo os autores, crimes como a divulgação de informações pessoais, o roubo de identidade e o cyberbullying têm efeitos devastadores na vida dos indivíduos, comprometendo tanto a sua confiança quanto a sua saúde mental. Com a internet, esses danos se multiplicam rapidamente, e as vítimas muitas vezes têm dificuldades em remover o conteúdo prejudicial. Nesse contexto, os autores ressaltam a importância de mecanismos legais que garantem não só a punição dos infratores, mas também a proteção das vítimas, permitindo-lhes restabelecer sua imagem e seu bem-estar.

Dessa maneira, uma invasão de dispositivos informáticos é um crime particularmente preocupante, visto que muitas vezes é uma porta de entrada para crimes ainda mais graves, como o roubo de dados bancários e informações pessoais sensíveis. Com o advento da Lei nº 14.155/2021, o Brasil buscou enfrentar esse tipo de crime de forma mais específica, mas a legislação ainda encontra limitações, principalmente quanto à caracterização da invasão e na dificuldade em comprovar a intenção criminosa. Em um ambiente virtual onde o anonimato e a multiplicidade de

dispositivos dificultam a identificação do autor, Milagre sugere que é fundamental aperfeiçoar as ferramentas tecnológicas e as técnicas de investigação para garantir uma proteção eficaz aos infratores (MILAGRE, 2021).

Assim, a cooperação internacional é uma peça-chave para a eficácia do combate aos crimes cibernéticos, uma vez que muitos crimes atuam de forma organizada e em redes que ultrapassam as fronteiras nacionais. A adesão à Convenção de Budapeste facilita o compartilhamento de informações e recursos entre países, mas os autores afirmam que, para ser eficaz, essa cooperação precisa estar alinhada com princípios de proteção de direitos e deve respeitar as diferentes legislações e culturas jurídicas. A convenção, apesar de seus benefícios, também exige que o Brasil adapte suas normas internacionais para atender às exigências e compromissos internacionais, o que pode ser um processo complexo e desafiador (CORRÊA; MONTEIRO NETO, 2023).

Por outro lado, Silva (2021) observa que a implementação das diretrizes da Convenção de Budapeste no Brasil é um passo importante, mas não suficiente para conter o avanço dos crimes cibernéticos. Ele ressalta que, além das adaptações legislativas, o Brasil precisa investir na formação de profissionais especializados em cibersegurança e no desenvolvimento de tecnologias de monitoramento e rastreamento digital. A criação de uma força-tarefa que inclui não apenas autoridades legais, mas também especialistas em tecnologia, pode ser uma solução eficaz para enfrentar o cibercrime, garantindo que o país tenha as condições aplicáveis para atuar de maneira preventiva e reativa frente às ameaças digitais (SILVA, 2021),

Corroborando com essa perspectiva, Edinilson Santos Vieira (2023) aborda que, para além da cooperação internacional e das mudanças legislativas, é fundamental que a sociedade esteja consciente dos riscos e tome medidas preventivas no uso da internet. Os autores defendem que campanhas educativas e a inclusão de conteúdos sobre segurança digital nas escolas e instituições públicas poderiam reduzir o impacto dos crimes cibernéticos, criando uma cultura de prevenção e cuidado, pois a luta contra o crime cibernético deve envolver não apenas as autoridades e o sistema legal, mas também a conscientização dos usuários, promovendo um uso mais seguro e responsável das tecnologias digitais.

4. AMBIENTE DIGITAL E OS DESAFIOS JURÍDICOS DA CONTEMPORANEIDADE

O ambiente digital trouxe transformações profundas para a sociedade, gerando desafios jurídicos que refletem a complexidade e rapidez com que as novas tecnologias impactam a vida cotidiana e as relações legais. De acordo com Maciel (2023) em um cenário onde a interação ocorre predominantemente em plataformas digitais e redes sociais, surgem questões sobre privacidade, proteção de dados, direitos autorais e responsabilidade das empresas que administram esses espaços virtuais.

O caráter transnacional da internet desafia os sistemas legais locais, pois os crimes e disputas que ocorrem no ambiente digital muitas vezes ultrapassam fronteiras, exigindo uma colaboração internacional que nem sempre é facilmente alcançada devido às diferenças nas leis e nos nossos interesses nacionais (TOCANTINS, 2024)

Nesse contexto, Giolo Júnior e Vilela (2024) discorrem que as legislações como o Regulamento Geral de Proteção de Dados (GDPR) na União Europeia e a Lei Geral de Proteção de Dados (LGPD) no Brasil representam passos significativos, mas ainda há a necessidade de harmonizar normas e fortalecer mecanismos de cooperação jurídica global. A evolução do direito digital mostra-se, assim, como um

processo contínuo de adaptação, que requer dos legisladores uma atualização constante frente às inovações tecnológicas e uma visão abrangente para antecipar e mitigar os impactos de um mundo cada vez mais conectado.

4.1 SISTEMA PROCESSUAL PENAL BRASILEIRO

O ambiente digital trouxe uma série de desafios ao sistema processual penal brasileiro, evidenciando a necessidade de uma adequação legislativa para lidar com crimes cibernéticos que, devido à sua natureza particular, escapam às definições e práticas do direito penal tradicional.

Para Ferreira (2021) o ordenamento jurídico brasileiro ainda é ineficaz na repressão e investigação desses crimes, devido à dificuldade em estabelecer provas e em identificar os infratores, que muitas vezes atuam de maneira anônima e global. A autora enfatiza que, apesar das tentativas de regulamentação, como as rupturas na Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, o Brasil ainda enfrenta dificuldades estruturais e legislativas que comprometem a efetividade do processo penal nesses casos.

Nessa linha pensamento, importa mencionar os ensinamentos de Brito (2020) ao afirmar que a recepção da Lei 12.737/2012, foi uma das primeiras leis no Brasil a abordar diretamente o crime cibernético, e ainda aponta que, embora tenha sido um avanço ao tipificar condutas específicas como a invasão de dispositivos informáticos, a lei possui limitações graves que torne sua aplicação ineficiente. Para Brito, a abrangência da lei é limitada e não acompanha a evolução constante dos crimes digitais, deixando várias práticas cibernéticas de fora do escopo penal, sendo necessário reformas contínuas e atualizações legislativas, algo que o autor considera essencial para que o sistema processual penal brasileiro possa acompanhar o ritmo da criminalidade digital e, assim, garantir uma proteção mais eficaz para os cidadãos no ambiente digital.

Por sua vez, Pompeu (2022) aprofunda uma análise sobre as limitações da Lei Carolina Dieckmann, destacando que a legislação envolve a complexidade dos crimes cibernéticos. Segundo os autores, a lei foi formulada em um contexto específico, motivada por um caso isolado de invasão e vazamento de dados pessoais de uma figura pública, sem um estudo mais abrangente sobre a influência dos crimes cibernéticos no Brasil. Para tanto, argumentam que, para que o sistema processual penal brasileiro seja realmente eficaz, é necessário que novas leis sejam criadas com uma abordagem mais holística e adaptada à realidade do ambiente digital, prevendo as diversas modalidades de crimes e as técnicas utilizadas pelos cibercriminosos.

Cabe mencionar a compreensão de Calixto, Facuri e Teles (2023) ao discutirem sobre a cooperação jurídica internacional e como isso é essencial para o combate aos crimes cibernéticos, tendo em vista que na maioria dos casos, esses crimes envolvem múltiplas jurisdições. Os autores apontam que, para que o sistema processual penal brasileiro seja capaz de atuar com efetividade no enfrentamento do crime cibernético, ele deve contar com uma estrutura sólida de cooperação com outros países, possibilitando o compartilhamento de provas e a troca de informações entre autoridades de diferentes nações. Entretanto, alertam que as faltas de um padrão internacional harmonizado, além das diferenças culturais e legais entre os países, representam obstáculos que o Brasil precisa superar para promover uma atuação mais assertiva e coordenada contra o crime cibernético.

Nesse ínterim, Ferreira (2021) explica que a dificuldade de obtenção de provas no ambiente digital, considerando que a volatilidade dos dados e o uso de redes descentralizadas dificultam a coleta de informações confiáveis que podem ser

utilizadas em processos penais. A autora critica o fato de o sistema processual penal brasileiro ainda estar ancorado em métodos tradicionais de investigação, muitas vezes ineficazes quando aplicados ao cibercrime. Para isso, é urgente a adaptação das técnicas de coleta e análise de provas, com o uso de ferramentas tecnológicas avançadas e a capacitação de agentes de segurança para que possam lidar com as especificidades da criminalidade digital.

O entendimento de Brito (2020) corrobora com o contexto abordada, pois propõe que o sistema processual penal brasileiro precisa integrar novas tecnologias e procedimentos investigativos que sejam compatíveis com o ambiente digital. O autor ainda observa que a ausência de especialização e de investimentos especializados em tecnologias de ponta limita a capacidade das autoridades de identificar e processar infratores de maneira eficaz.

Nesse sentido, torna-se importante uma revisão das avaliações aplicadas aos crimes cibernéticos, uma vez que as penas determinantes pela legislação brasileira não refletem a gravidade dos danos causados por esses delitos. Esse cenário implica em crimes como o vazamento de dados pessoais e financeiros que devem ser tratados com maior rigor, considerando o impacto devastador que pode ter sobre as vítimas. Nota-se que, a legislação penal necessita de uma urgente reforma para de fato oferecer punições assertivas e desestimular a prática de crimes no ambiente digital, algo que também contribuirá para fortalecer a confiança da população no sistema de justiça (POMPEU, 2022).

Portanto, a luta contra os crimes cibernéticos demanda um esforço conjunto que requer não apenas avanços legislativos e tecnológicos, mas também uma conscientização da sociedade sobre os riscos e a importância de adotar práticas seguras no uso da internet. Essa problemática desemboca no sistema processual penal que deve ser encarado a partir de uma abordagem multidisciplinar, ou seja, que tenha a contribuição de vários setores da sociedade e um trabalho que envolva cooperação internacional alinhado aos desafios do ambiente digital (CALIXTO; FACURI; TELES, 2023).

4.2 ATUAÇÃO DO PODER JUDICIÁRIO BRASILEIRO E A RESPONSABILIZAÇÃO PENAL DE AGENTES ESTRANGEIROS

Segundo Israel (2020, p. 79) as transformações que a Internet vem sofrendo passam a demandar novas formas de aplicação da soberania em nível interno, que impactam inevitavelmente as relações externas. Por essa razão, a atuação do Poder Judiciário brasileiro no combate a cibernéticos desbrava um cenário de constantes desafios, diante de infrações penais que decorram de agentes estrangeiros, cuja responsabilização penal é complexa e exige adaptações legais e operacionais.

Nessa linha abordagem, observa Santana (2021) que a legislação penal brasileira passou por uma evolução importante, mas ainda insuficiente para acompanhar o dinamismo do ambiente digital, onde crimes de diversas naturezas podem ser crimes por indivíduos ou grupos de fora do território nacional. Ele argumenta que a globalização dos crimes cibernéticos exige do Poder Judiciário brasileiro uma capacidade de resposta que transcenda as fronteiras tradicionais, levando em conta a cooperação internacional como uma ferramenta necessária para lidar com o crime cibernético.

Araújo (2021) complementa essa visão ao afirmar que o direito penal aplicado aos crimes virtuais enfrenta limitações severas quando o crime é praticado por agentes estrangeiros. A ausência de uma supervisão global unificada dificulta a aplicação de avaliações a cibercriminosos que atuam a partir de outros países,

utilizando-se de tecnologias e redes que dificultam a identificação e a proteção. O autor ainda destaca que a atuação do Poder Judiciário depende em muitos momentos da colaboração de outras nações e da adaptação dos processos investigativos e judiciais à realidade transnacional dos crimes digitais, algo que considera essencial para garantir a eficácia da responsabilização penal.

Considerando a discussão, insta salientar que um dos principais entraves para a responsabilização penal de agentes estrangeiros está na dificuldade da investigação cibernética, que requer tecnologia avançada e uma integração de esforços entre diferentes jurisdições, visto que a natureza volátil dos dados e as técnicas de anonimato utilizadas pelos criminosos tornam o processo de identificação e coleta de provas extremamente complexo, mesmo com a cooperação internacional (SILVA, 2022).

Dessa forma, a cooperação jurídica internacional é um dos pilares na atuação do Judiciário brasileiro para o enfrentamento do crime cibernético, tendo em vista que o Brasil tem se esforçado para firmar tratados e participar de convenções internacionais que facilitam o compartilhamento de informações e a realização de investigações conjuntas, como a Convenção de Budapeste. Contudo, essa cooperação enfrenta barreiras, como a incompatibilidade legislativa entre países e a falta de um padrão global sobre crimes cibernéticos, razão pela qual o Poder Judiciário brasileiro deve intensificar suas parcerias internacionais e buscar uma atuação mais integrada para responsabilizar penalmente agentes estrangeiros envolvidos em crimes cibernéticos (CALIXTO; FACURI; TELES, 2023).

De modo similar Santana (2021) aponta que a ausência de mecanismos eficazes para identificar e punir agentes estrangeiros coloca em risco a soberania do Brasil no ambiente digital, uma vez que muitos crimes cometidos por estrangeiros afetam diretamente a população e as instituições brasileiras. Ressalta ainda, a importância de uma abordagem mais robusta e proativa do Judiciário, que deve ser capaz de aplicar a legislação nacional de forma adaptada ao contexto digital, com vistas à proteção dos cidadãos e das empresas nacionais, sugerindo que o fortalecimento das competências internas e a criação de leis específicas para crimes cibernéticos de impacto transnacional podem ser estratégias eficazes para enfrentar o problema.

Embora a responsabilização de agentes estrangeiros dependa de fatores externos, como a cooperação de outros países, o Poder Judiciário brasileiro deve continuar aprimorando a legislação e as práticas jurídicas para dar uma resposta exemplar nos casos de crimes cibernéticos que afetam o país, pois isso incluiria penas mais severas para cibercriminosos e uma abordagem mais rigorosa na aplicação das leis, demonstrando o compromisso do Brasil em proteger seu ambiente digital (ARAÚJO, 2021).

Por outro lado, Silva (2022) coloca em pauta a necessidade de aprimoramento nas técnicas de investigação para aumentar a eficácia do Judiciário em casos de crimes cibernéticos transnacionais. O autor sugere que, para responsabilizar penalmente os agentes estrangeiros, é essencial que o Brasil invista em capacitação tecnológica e na formação de profissionais especializados em cibersegurança e investigação digital. A falta de preparo técnico nas investigações de crimes digitais representa uma lacuna que compromete a eficiência do sistema de justiça e enfraquece o potencial de resposta do país frente ao cibercrime global (SILVA, 2022).

Desse modo, a questão da responsabilidade penal dos agentes estrangeiros vai além da aplicação de leis nacionais, exigindo um compromisso global com a segurança cibernética. Nesse contexto, o Brasil precisa participar de pesquisas

internacionais e adotar políticas que permitam uma integração mais eficaz entre os países. Essa atuação integrada do sistema de justiça com outras nações corrobora para aprimoramento das práticas processuais, acarretando uma prestação jurisdicional mais eficiente na responsabilização de agentes estrangeiros, e assim proporcionando maior compromisso com a justiça e a segurança digital (CALIXTO; FACURI; TELES, 2023).

5. LIMITES JURÍDICOS NO ENFRENTAMENTO À CRIMINALIDADE VIRTUAL E A COOPERAÇÃO INTERNACIONAL

Os limites jurídicos no enfrentamento à criminalidade virtual representam um dos maiores desafios contemporâneos para o direito penal e a cooperação internacional. De acordo com Sousa (2023) o crescimento exponencial do uso da internet, os crimes cibernéticos também se diversificaram, aumentando a vulnerabilidade das vítimas e ampliando a necessidade de uma resposta jurídica eficaz. Por conseguinte, o autor aponta que o controle penal encontra barreiras significativas para lidar com esses crimes, principalmente devido à dificuldade em rastrear e identificar os responsáveis, que muitas vezes se escondem atrás de tecnologias que mascaram a identidade e a localização. A globalidade da internet torna os limites territoriais do direito penal ineficazes, exigindo que os Estados ajustem suas legislações e aprimorem a cooperação com outros países.

Nesse viés, esclarece Zambonato (2022) que a legislação brasileira tem avançado no combate aos crimes cibernéticos, buscando acompanhar a complexidade do ambiente digital com leis mais específicas, como a Lei nº 12.737/2012. O autor ressalta que, embora tais avanços sejam importantes, a legislação ainda apresenta lacunas que limitam a eficácia do combate à criminalidade virtual, suscitando em sua discussão que é necessário atualizar constantemente as normas penais, dada a rápida evolução das tecnologias e das táticas utilizadas pelos infratores. Assim, um dos principais desafios jurídicos é justamente adaptar-se à natureza dinâmica da internet, onde novas modalidades de crimes surgem com rapidez e dificultam a aplicação das leis.

Acerca desse assunto, nota-se que além das limitações legais, o Brasil enfrenta o desafio de alinhar o seu ordenamento jurídico com os padrões internacionais, considerando o contexto da criminalidade virtual. Sendo assim, os países devem adotar uma postura de cooperação para lidar com os crimes cibernéticos, que frequentemente ultrapassam as fronteiras nacionais. Destaca ainda o autor que a diversidade das legislações e a ausência de um consenso internacional sobre como punir esses crimes criam obstáculos para uma ação conjunta eficaz. Segundo ele, o Brasil deve se esforçar para harmonizar suas práticas com as normas internacionais, de modo a fortalecer sua capacidade de cooperação e, assim, garantir que os crimes cibernéticos sejam devidamente investigados e punidos (GUIMARÃES, 2024).

Em vista disso, Kilian (2020) afirma que a eficácia da legislação brasileira no enfrentamento aos crimes cibernéticos depende de uma abordagem integrada, que inclui tanto o aprimoramento das leis nacionais quanto à cooperação com outros países. Ele explica que a complexidade dos crimes virtuais exige uma articulação entre as nações, pois esses crimes são muitas vezes cometidos por redes organizadas que atuam de forma descentralizada e global. Nessa linha de pensamento, defende que o Brasil precisa avançar na criação de tratados e acordos de cooperação jurídica que possibilitem a troca de informações e o suporte mútuo em investigações, de forma a garantir uma resposta mais eficaz ao crime cibernético.

Por outro lado, Lima (2024) apresenta sua preocupação quanto aos desafios das investigações que envolvam praticas cibernéticas, que incluem a volatilidade dos dados e as técnicas de anonimato utilizadas pelos criminosos. Observa em sua análise que a natureza intangível das provas digitais e a rapidez com que os dados podem ser eliminados ou modificados representam obstáculos significativos para a investigação penal. O sistema jurídico brasileiro precisa se adaptar para enfrentar esses desafios, o que inclui o desenvolvimento de técnicas investigativas avançadas e a capacitação de profissionais especializados em cibersegurança e rastreamento digital. Sem esses avanços, o enfrentamento da criminalidade virtual continuará a ser ineficaz, limitando a capacidade do sistema de justiça de responsabilizar os infratores (LIMA, 2024).

Assim, os crimes virtuais representam uma ameaça crescente à segurança pública e à integridade dos indivíduos e das instituições. Logo, constata-se que o ordenamento jurídico brasileiro ainda carece de mecanismos eficientes para prevenir e punir os cibercriminosos, e que é necessário um esforço contínuo para aprimorar as legislações e torná-las compatíveis com a realidade digital, visto que a adoção de medidas preventivas e punitivas mais rigorosas poderia ajudar a dissuadir potenciais infratores e aumentar a segurança no ambiente virtual (LOPES; LOPES, 2023).

A cooperação internacional é apontada por Dobler (2023) como um elemento central para o enfrentamento da criminalidade virtual no Brasil. Argumentaram que, sem a colaboração de outros países, a responsabilização penal dos cibercriminosos é praticamente inviável, dada a facilidade com que eles operam em diferentes localidades e se escondem atrás de tecnologias de anonimato. Os autores defendem que o Brasil deve intensificar sua participação em tratados e acordos multilaterais, como a Convenção de Budapeste, para fortalecer a cooperação em matéria penal e garantir que as investigações possam cruzar fronteiras sem impedimentos legais.

Sousa (2023) reforça a importância de consideração do papel da vítima nos crimes cibernéticos, discutindo que, no ambiente digital, as vítimas em muitos casos enfrentam dificuldades para ver seus direitos assegurados. Salienta-se que muitos crimes cibernéticos têm consequências na vida das vítimas, afetando sua confiança, saúde mental e até sua segurança física. Porém, o sistema jurídico atual ainda é insuficiente para fornecer uma proteção eficaz às vítimas de crimes virtuais, o que evidencia a necessidade de reformas legais que ampliem o suporte e a assistência para aqueles que sofrem com a criminalidade digital, sendo que uma maior atenção às necessidades das vítimas também contribuiria para fortalecer a resposta penal contra os infratores.

Dessa forma, uma legislação que ampliasse o alcance das novas modalidades de crimes cibernéticos, os quais se sofisticaram e exigem uma atuação rápida e precisa do sistema de justiça. Por essa razão, a criação de leis específicas para crimes cibernéticos é uma medida urgente, pois as normas tradicionais de direito penal não são suficientes para enfrentar a complexidade desses crimes. Essa inclusão de novas categorias penais e a definição de penas mais rigorosas poderiam ajudar a reduzir a criminalidade virtual no Brasil, ao mesmo tempo que enviariam uma mensagem de comprometimento do país com a segurança digital (ZAMBONATO, 2022).

Guimarães (2024) acrescenta que a criminalidade virtual desafia os conceitos tradicionais de jurisdição e territorialidade, uma vez que os cibercriminosos podem atuar de qualquer lugar do mundo e afetar vítimas em diversos países simultaneamente. Ele aponta que o Brasil precisa adaptar seu sistema jurídico para lidar com essa realidade, ou que inclui a criação de mecanismos que permitam a

aplicação extraterritorial das leis e a cooperação com órgãos de justiça estrangeiros. Guimarães adverte que essa adaptação é fundamental para que o país possa combater a criminalidade virtual de maneira eficaz e proteger os cidadãos no ambiente digital.

Para tanto, argumenta Kilian (2020) que apesar das limitações da legislação brasileira, é possível observar avanços na maneira como o país aborda o combate ao crime cibernético. Ele afirma que, além de aprimorar as leis, é essencial investir em capacitação e em infraestrutura tecnológica, de modo a garantir que o sistema de justiça brasileiro tenha as ferramentas possíveis para enfrentar o crime cibernético. A criação de equipes especializadas e o desenvolvimento de centros de cibersegurança são medidas que poderiam fortalecer o enfrentamento à criminalidade virtual, proporcionando uma resposta mais ágil e eficaz aos desafios impostos pelo ambiente digital.

Em síntese, Dobler (2023) enfatiza que, para que a cooperação internacional seja realmente eficaz, é necessário que o Brasil assuma um papel ativo nas discussões globais sobre cibersegurança e cooperação jurídica. Eles defendem que o país deve trabalhar para construir uma rede de parcerias internacionais e desenvolver normas comuns que facilitem a responsabilização penal de crimes virtuais. Para os autores, essa postura proativa não apenas fortalece a segurança digital do Brasil, mas também contribui para a criação de um ambiente online mais seguro e justo, onde as fronteiras físicas deixam de ser um obstáculo à justiça e à proteção das vítimas de crimes cibernéticos.

6. CONSIDERAÇÕES FINAIS

Os crimes cibernéticos cometidos por agentes estrangeiros contra vítimas brasileiras representam um desafio significativo para o sistema jurídico do Brasil, que ainda precisa se adaptar às novas realidades impostas pelo ambiente virtual. A natureza transnacional desses crimes torna complexa a aplicação das leis nacionais, exigindo uma abordagem jurídica que transcenda as fronteiras territoriais e seja capaz de lidar com as peculiaridades do ciberespaço.

A dificuldade em estabelecer a jurisdição adequada, somada à necessidade de harmonização legislativa entre diferentes países, é uma das principais barreiras enfrentadas pelos sistemas de justiça na tentativa de investigar, processar e punir os infratores de maneira eficiente.

Outro obstáculo importante reside na velocidade com que as tecnologias digitais evoluem, o que demanda uma constante atualização das leis para acompanhar as novas formas de infrações cibernéticas. A Lei nº 12.737/2012, apesar de representar um avanço para o direito brasileiro, mostra-se limitada diante da sofisticação dos crimes cibernéticos atuais, notadamente no que tange à invasão de dispositivos informáticos por agentes estrangeiros.

O dinamismo do ambiente digital exige que as legislações sejam flexíveis e abrangentes, possibilitando a adaptação rápida às novas ameaças virtuais, sem perder de vista os direitos fundamentais dos cidadãos. Assim, o Brasil precisa avançar em sua legislação e desenvolver mecanismos jurídicos mais robustos para enfrentar essa modalidade de criminalidade de forma eficaz.

A cooperação internacional é um elemento imprescindível para o sucesso na investigação e punição de crimes cibernéticos transnacionais. Sem uma colaboração efetiva entre os países, as investigações podem ser prejudicadas, pois as provas muitas vezes estão armazenadas em servidores estrangeiros ou envolvem criminosos que operam de fora do país.

A falta de tratados internacionais abrangentes e de uma participação mais ativa do Brasil em convenções como a de Budapeste limita as possibilidades de uma cooperação eficiente, atrasando processos e favorecendo a impunidade. O fortalecimento dos acordos internacionais e a participação em fóruns globais de discussão sobre cibercrime são medidas essenciais para promover uma integração mais eficaz entre os países no combate ao crime cibernético.

O processo de investigação de crimes cibernéticos também enfrenta desafios técnicos consideráveis. A coleta de provas digitais, a identificação de criminosos que utilizam técnicas de ocultação como criptografia e redes de anonimato, e a necessidade de rapidez na preservação de dados são aspectos críticos que dificultam a atuação das autoridades brasileiras.

Essas dificuldades tornam urgente a modernização das ferramentas tecnológicas disponíveis para os órgãos de investigação e a capacitação dos profissionais que atuam na área de cibersegurança e justiça. Investir em tecnologia e expertise é fundamental para que o Brasil possa acompanhar as inovações tecnológicas e desenvolver um sistema de justiça mais preparado para lidar com crimes cibernéticos.

O impacto dos crimes cibernéticos transcende a esfera jurídica e atinge diretamente as vítimas, que muitas vezes enfrentam danos financeiros, psicológicos e à sua reputação. A dificuldade em responsabilizar agentes estrangeiros agrava a sensação de vulnerabilidade das vítimas, uma vez que a justiça nem sempre consegue oferecer uma resposta rápida e eficaz.

As diferenças nas legislações de cada país, a burocracia nos processos de cooperação internacional e a ausência de uma legislação suficientemente abrangente no Brasil tornam o processo judicial lento e muitas vezes ineficaz. As vítimas, por sua vez, ficam desamparadas e, muitas vezes, sem a reparação adequada pelos danos sofridos.

Diante desse cenário, constata-se que a superação dos desafios jurídicos relacionados aos crimes cibernéticos cometidos por agentes estrangeiros requer uma ação coordenada entre diferentes frentes. É necessário fortalecer as leis internas, atualizar as normas vigentes e ampliar a participação do Brasil em acordos internacionais que facilitem a troca de informações e a cooperação jurídica entre os países. Além disso, é fundamental que o sistema de justiça esteja preparado para lidar com a natureza técnica e transnacional dos crimes cibernéticos, adotando medidas preventivas e reativas que sejam eficazes e ágeis.

O desenvolvimento de uma legislação mais adaptada à realidade digital e a criação de estruturas de cooperação internacional mais sólidas são passos essenciais para garantir a responsabilização de criminosos virtuais, independentemente de sua localização geográfica.

A atuação conjunta entre países, aliada ao uso de tecnologias de ponta e à capacitação de profissionais, poderá fornecer as bases para um sistema jurídico mais eficiente e capaz de enfrentar os desafios impostos pelos crimes cibernéticos. Somente com esses esforços será possível oferecer uma resposta eficaz às vítimas e assegurar que a justiça seja aplicada, mesmo em um ambiente tão complexo como o ciberespaço.

Por fim, os desafios enfrentados pelo Brasil no julgamento de crimes cibernéticos cometidos por agentes estrangeiros revelam a necessidade de uma transformação tanto na esfera jurídica quanto na tecnológica. O país precisa se posicionar de maneira mais ativa no cenário internacional, participando de discussões e convenções globais sobre cibercrime, ao mesmo tempo em que fortalece suas leis

e suas instituições internas para lidar com essas novas formas de criminalidade. A cooperação internacional, a modernização legislativa e o investimento em tecnologia são os pilares fundamentais para o enfrentamento eficaz dos crimes cibernéticos, garantindo que a justiça prevaleça, mesmo diante das barreiras impostas pelo mundo digital.

Referências

ALBUQUERQUE, Felipe; TIBURCIO, Carmen. Territorialidade, jurisdição e internet: alguns aspectos de direito internacional privado. **Revista Eletrônica de Direito Processual,** v. 24, n. 3, 2023. ISSN 1982-7636. Disponível em: https://www.e-publicacoes.uerj.br/redp/article/view/79553. Acesso em: 03 nov. 2024.

ALVES, Leonardo Barreto Moreira. **Processo penal parte geral**. 14 ed. São Paulo: JusPODIVM, 2024.

ARAÚJO, Claudio Rodrigues. **Análise da aplicação do direito penal nos crimes virtuais**. Belo Horizonte: Expert, 2021. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=bX3LEAAAQBAJ&oi=fnd&pg=PA11&dq=ARAUJO,+Claudio+Rodrigues.+An%C3%A1lise+da+aplica%C3%A7%C3%A3o+do+direito+penal+nos+crimes+virtuais.+Expert+Editora,+2021.&ots=deGZAhsicM&sig=Fg6XQPLbYAfJui-NDciUNF8HhJE#v=onepage&q=ARAUJO%2C%20Claudio%20Rodrigues.%20An%C3%A1lise%20da%20aplica%C3%A7%C3%A3o%20do%20direito%20penal%20nos%20crimes%20virtuais.%20Expert%20Editora%2C%202021.&f=false. Acesso em: 31 de out. 2024.

BRITO, Marcelo Matos. **Crimes cibernéticos e a recepção da lei no 12.737/2012 no Brasil**. 2020. 19 f. Trabalho de Conclusão de Curso (Especialização Latu Sensu em Ciências Criminais), Universidade Católica de Salvador, Salvador, 2020. Disponível em: https://ri.ucsal.br/items/1ded7eeb-dd99-42ae-ba28-6314a1136158. Acesso em: 31 out. 2024.

CALIXTO, Tharynne Marcela Barbosa; FACURI, Antônio Carlos Gomes; TELES, Fernando Hugo Miranda. As relações de cooperação jurídica internacional no combate às práticas de cibercrimes. **Revista do Ministério Público Militar**, v. 50, n. 39, p. 235-244, 2023. Disponível em: https://revista.mpm.mp.br/rmpm/article/view/148. Acesso em: 31 de out. 2024.

CAPEZ, Fernando. **Curso de direito penal**. 20 ed. São Paulo: Saraiva, 2013.

CORRÊA, Isadora Donza; MONTEIRO NETO, João Araújo. A adesão do Brasil à Convenção de Budapeste e o enfrentamento do Cibercrime: entre a Cooperação Internacional e a expansão do Direito Penal. **Revista Eletrônica Direito & TI**, v. 1, n. 16, p. 32-60, 2023. Disponível em: https://direitoeti.emnuvens.com.br/direitoeti/article/view/155. Acesso em: 31 out. 2024.

CUNHA, Rogério Sanches. **Código penal para concursos**. 12 ed. Salvador: JusPODIVM, 2019.

DOBLER, Kellen. **Cooperação internacional em matéria penal e o crime cibernético no Brasil**. 2023. 159 f. Dissertação (Mestrado em Direito), Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2023. Disponível em: https://www.bdtd.uerj.br:8443/handle/1/22382#preview-link0. Acesso em 31 de out. 2024.

FERREIRA, Sarah Pereira. **Crimes cibernéticos**: a ineficácia da legislação brasileira. 2021. 31 f. Trabalho de Conclusão de Curso (Graduação em Direito), Pontifícia Universidade Católica de Goiás, Goiânia, 2021. Disponível em: https://repositorio.pucgoias.edu.br/jspui/handle/123456789/1709. Acesso em: 31 out. 2024.

GOMES, Walyson Milhomem Souza de; MEDRADO, Lucas Cavalcante. Crimes cibernéticos uma ponderação sobre a Lei 14.155 de 2021 aplicável ao crime de estelionato virtual. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, *[S. l.]*, v. 9, n. 9, p. 1870–1894, 2023. Disponível em: https://periodicorease.pro.br/rease/article/view/11321#:~:text=Com%20base%20nos%20resultados%20obtidos,sujeitos%20ativos%20do%20estelionato%20virtual. Acesso em: 03 nov. 2024.

ISRAEL, Carolina Batista. Território, jurisdição e ciberespaço: entre os contornos westfalianos e a qualidade transfronteiriça da Internet. **Geousp: Espaço e Tempo (On-line)**, v. 24, n. 1, p. 69-82, abr. 2020. ISSN 2179-0892. Disponível em: https://www.revistas.usp.br/geousp/. Acesso em 03 nov. 2024.

GIOLO JÚNIOR, Cildo; VILELA, Maria Eduarda Marçal. Lei geral de proteção d dados (LGDP) e general data protection (GDPR): uma análise entre os principais elementos das legislações e suas sanções aos casos de vazamentos de dados. **Revista de Iniciação Científica e Extensão da Faculdade de Direito de Franca**, v. 8, n. 1, p 637-661, dez. 2023 ISSN 2675-0104. Disponível em: https://revista.direitofranca.br/index.php/icfdf/article/view/1516. Acesso em: 03 nov. 2024.

GUIMARÃES, Pedro Vinicius. **A Criminalidade virtual e os desafios do direito brasileiro face o avanço dos crimes cibernéticos**. 2024. 32 f. Trabalho de Conclusão de Curso (Graduação em Direito), Pontifícia Universidade Católica de Goiás, Goiânia. 2024. Disponível em: https://repositorio.pucgoias.edu.br/jspui/handle/123456789/7549. Acesso em: 31 out. 2024.

JÊIOR, Júlio César Alexandre. Cibercrime: um estudo acerca do conceito de crimes informáticos. **Revista Eletrônica da Faculdade de Direito de Franca**, v. 14, n. 1, p. 341-351, 2019. Disponível em: https://revista.direitofranca.br/index.php/refdf/article/view/602. Acesso em: 31 out. 2024.

KILIAN, Jean. **Crimes cibernéticos uma abordagem jurídica diante da eficácia na legislação brasileira**. 2020. 65 f. Trabalho de Conclusão de Curso (Graduação

em Direito), Universidade de Santa Cruz do Sul, Santa Cruz do Sul. 2020. Disponível em: https://repositorio.unisc.br/jspui/handle/11624/2993. Acesso em: 31 out. 2024.

LIMA, Douglas Magno Fernandes do Nascimento. **Os desafios da investigação nos crimes cibernéticos**. 2024. 74 f. Trabalho de Conclusão de Curso (Graduação em Direito), Universidade Federal da Paraíba, Santa Rita, 2024. Disponível em: https://repositorio.ufpb.br/jspui/handle/123456789/31393. Acesso em: 31 out. 2024.

LOPES, Marciano Pereira; LOPES, José Augusto Bezerra. Crimes virtuais no ordenamento jurídico brasileiro. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, v. 9, n. 8, p. 462-472, 2023. Disponível em: https://periodicorease.pro.br/rease/article/view/10850. Acesso em: 31 out. 2024.

MACIEL, Natalia Ferraz de Menezes. A globalização das plataformas digitais: análise sobre a necessidade de regulamentação dessa ferramenta. **Revista Foco**, v. 16, n. 10, p. 01-20, 2023. Disponível em: https://ojs.focopublicacoes.com.br/foco/article/view/3092. Acesso em: 03 nov. 2024.

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. Disponível em: https://ojs.journalsdg.org/jlss/article/view/51. Acesso em: 31 out. 2024.

MILAGRE, José Antônio. Lei de crimes informáticos (14.155/2021): aspectos técnicos controvertidos e critérios para caracterização do crime de “invasão de dispositivo informático”. *In*: **Blog José Antônio Milagre Advocacia**, 31 jul. 2021. Disponível em: https://direitodigital.adv.br/artigos/lei-de-crimes-informaticos-14-155-2021-aspectos-tecnicos-controvertidos-e-criterios-para-caracterizacao-do-crime-de-invasao-de-dispositivo-informatico/?print=print. Acesso em: 31 out. 2024.

NAME, Luciana de Almeida Pupulin. **Crimes cibernéticos e seus impactos na imagem do indivíduo**. 2023. 40 f. Trabalho de Conclusão de Curso (Graduação em Direito), Pontifícia Universidade Católica de Goiás, Goiânia, 2023. Disponível em: https://repositorio.pucgoias.edu.br/jspui/handle/123456789/5764. Acesso em: 31 out. 2024.

POMPEU, Ana Luiza Brandão Calil. **Crimes cibernéticos**: a ineficácia da lei carolina dieckmann. 2022. 41 f. Trabalho de Conclusão de Curso (Graduação em Direito), Faculdade Facmais, Inhumas, 2022. Disponível em: http://65.108.49.104/handle/123456789/509. Acesso em: 31 out. 2024.

SANTANA, Roque Felipe da Silva. **Crimes cibernéticos**: análise evolutiva da legislação penal brasileira e seus desafios. 2021. 24 f. Trabalho de Conclusão de Curso (Graduação em Direito), Universidade Católica do Salvador, Salvador, 2021. Disponível em: https://ri.ucsal.br/items/eacce13d-1953-456e-af9a-28ae647dd351. Acesso em: 31 out. 2024.

SILVA, Dickson Carvalho Gonçalves da. **Crimes cibernéticos**: limites e desafios da investigação. 2022. 68 F. Trabalho de Conclusão de Curso (Graduação em Direito),

Centro Universitário – UNDB, São Luís, 2022. Disponível em: http://repositorio.undb.edu.br/handle/areas/834. Acesso em: 31 out. 2024.

SILVA, Matheus Giboski Moreira da. **A convenção de Budapeste e a cooperação jurídica internacional como ferramentas essenciais na repressão aos crimes cibernéticos no Brasil**. 2021. 84 f. Trabalho de Conclusão de Curso (Graduação em Direito), Universidade do Vale do Rio dos Sinos, São Leopoldo, 2021. Disponível em: https://repositorio.jesuita.org.br/bitstream/handle/UNISINOS/11105/Matheus%20Giboski%20Moreira%20da%20Silva.pdf?sequence=1. Acesso em 31 out. 2024.

SOUSA, Lucas Queiroga Nóbrega de. **Análise crítica do papel da vítima nos crimes cibernéticos e dos desafios do controle penal**. 2023. 76 f. Trabalho de Conclusão de Curso (Graduação em Direito), Universidade Federal da Paraíba, Santa Rita, 2023. Disponível em: https://repositorio.ufpb.br/jspui/handle/123456789/29440. Acesso em: 31 out. 2024.

TOCANTINS, Hortência Matos. Crimes cibernéticos na atualidade: desafios e impactos na sociedade moderna. **JusBrasil**, [2024]. [não paginado]. Disponível em: https://www.jusbrasil.com.br/artigos/crimes-ciberneticos-na-atualidade-desafios-e-impactos-na-sociedade-moderna/2104354886?_gl=1*1nkxaoi*_gcl_au*OTAyNDAzMzA3LjE3MjYyNzczMjM.*_ga*Nzc1ODY5NzkxLjE2Nzg3MzYwMzM.*_ga_QCSXBQ8XPZ*MTczMDkxNDk5MC41OS4wLjE3MzA5MTQ5OTAuNjAuMC4w. Acesso em: 31 out. 2024.

VIEIRA, Edinilson Santos. **Crimes cibernéticos**. [*S. l.*]: Viseu, [2023]. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=NVu5EAAAQBAJ&oi=fnd&pg=PT4&dq=VIEIRA,+Edinilson+Santos.+Crimes+Cibern%C3%A9ticos.+Viseu,+2023.&ots=GmhVwE29bm&sig=vCHbbPsmDLDtFJUdCbax8p0JOGI#v=onepage&q=VIEIRA%2C%20Edinilson%20Santos.%20Crimes%20Cibern%C3%A9ticos.%20Viseu%2C%202023.&f=false. Acesso em: 31 out. 2024.

VIEIRA, Maria Eduarda. **A adesão do Brasil a convenção de Budapeste e a correção das deficiências legislativas quanto aos crimes cibernéticos.** 2023. 79 f. Trabalho de Conclusão de Curso (Graduação em Direito), Universidade Federal de Santa Catarina, Florianópolis, 2023. Disponível em: https://repositorio.ufsc.br/handle/123456789/248821. Acesso em: 03 out. 2024.

ZAMBONATO, Matheus Schultz. **Avanços da legislação brasileira no combate aos crimes cibernéticos**. 2022. 50 f. Trabalho de Conclusão de Curso (Graduação em Direito), Universidade Federal do Rio Grande do Sul, Porto Alegre, 2022. Disponível em: https://lume.ufrgs.br/handle/10183/252036. Acesso em: 31 out. 2024.