

UNILEÃO
CENTRO UNIVERSITÁRIO DOUTOR LEÃO SAMPAIO
CURSO DE GRADUAÇÃO EM DIREITO

KAREN SANTOS DE OLIVEIRA

**CRIMES NA ERA DIGITAL: Análise da Fragilidade do Ordenamento Jurídico em
Relação aos Crimes Praticados em Ambiente Virtual**

JUAZEIRO DO NORTE-CE
2024

KAREN SANTOS DE OLIVEIRA

**CRIMES NA ERA DIGITAL: Análise da Fragilidade do Ordenamento Jurídico em
Relação aos Crimes Praticados em Ambiente Virtual**

Trabalho de Conclusão de Curso – *Artigo Científico*,
apresentado à Coordenação do Curso de Graduação em
Direito do Centro Universitário Doutor Leão Sampaio,
em cumprimento às exigências para a obtenção do grau
de Bacharel.

Orientador: Prof. Me. Francisco Thiago da Silva
Mendes.

KAREN SANTOS DE OLIVEIRA

**CRIMES NA ERA DIGITAL: Análise da Fragilidade do Ordenamento Jurídico em
Relação aos Crimes Praticados em Ambiente Virtual**

Este exemplar corresponde à redação final aprovada do
Trabalho de Conclusão de Curso de KAREN SANTOS
DE OLIVEIRA.

Data da Apresentação: 26/06/2024

BANCA EXAMINADORA

Orientador: PROF. ME. FRANCISCO THIAGO DA SILVA MENDES/ UNILEÃO

Membro: PROF. FRANCISCO GLEDISON LIMA ARAÚJO/ UNILEÃO

Membro: PROF. JOSÉ BOAVENTURA FILHO/ UNILEÃO

JUAZEIRO DO NORTE-CE
2024

CRIMES NA ERA DIGITAL: Análise da Fragilidade do Ordenamento Jurídico em Relação aos Crimes Praticados em Ambiente Virtual

Karen Santos de Oliveira¹
Francisco Thiago da Silva Mendes²

RESUMO

A pesquisa em questão é fruto de estudos voltados à análise da fragilidade do sistema jurídico brasileiro no enfrentamento dos crimes cibernéticos. O objetivo principal é analisar os crimes cibernéticos e seu crescimento devido à ausência de legislação eficaz, que se mostra insuficiente na regulamentação das infrações, uma vez que as normas existentes não acompanharam a evolução desses delitos. Os objetivos específicos incluem explicar a conceituação dos crimes cibernéticos, detalhar a evolução desses crimes em contraste com a defasagem normativa, sintetizar suas categorias e características, além de apresentar os desafios relativos à investigação criminal e propor possíveis soluções para o problema em questão. Para tanto, estruturou-se o artigo de modo a explorar o tema de maneira temática, dividindo-o em três segmentos: inicialmente, discorre sobre o surgimento dos crimes virtuais, delineando seu histórico e conceituação. Posteriormente, descreve as categorias de crimes virtuais. E, por fim, aborda a necessidade de adaptação do ordenamento jurídico aos delitos característicos da era digital. A metodologia adotada baseou-se em revisões bibliográficas pertinentes ao tema.

Palavras Chave: Crimes virtuais. Crimes Cibernéticos. Leis.

¹Graduanda do Curso de Direito do Centro Universitário Doutor Leão Sampaio/ Unileão. E-mail: kaah-2015@outlook.com.

²Professor Orientador. Mestre em Direito das Empresas. Pós-graduado em Direito Penal e Criminologia. Professor de Direito Penal e Empresarial. E-mail: thiagomendes@leãosampaio.edu.br

ABSTRACT

The research in question is the result of studies aimed at analyzing the fragility of the Brazilian legal system in combating cybercrimes. The main objective is to analyze cybercrimes and their growth due to the lack of effective legislation, which is insufficient in regulating infractions, since existing standards have not kept up with the evolution of these crimes. The specific objectives include explaining the conceptualization of cybercrimes, detailing the evolution of these crimes in contrast to the regulatory gap, synthesizing their categories and characteristics, in addition to presenting the challenges related to criminal investigation and proposing possible solutions to the problem in question. To this end, the article was structured to explore the topic in a thematic way, dividing it into three segments: initially, it discusses the emergence of virtual crimes, outlining their history and conceptualization. Subsequently, it describes the categories of virtual crimes. And, finally, it addresses the need to adapt the legal system to crimes characteristic of the digital era. The methodology adopted was based on bibliographical reviews relevant to the topic.

Keywords: Virtual. crimes. Cyber Crimes. Laws.

1 INTRODUÇÃO

A compreensão da violência na contemporaneidade demanda uma avaliação de conceitos que são percebidos como problemáticos tanto para a sociedade brasileira quanto para a comunidade internacional. Os índices de crimes virtuais registrados e as denúncias apresentam um aumento significativo, conforme indicam os dados da Ouvidoria Nacional de Direitos Humanos (SINDH), que não só apontam para um crescimento no número de vítimas de violência, mas também para a diversificação das formas de violência e exploração no meio virtual. Isso torna imperativa uma abordagem que busque métodos de maior vigilância por parte do Poder Público, da família e da comunidade (CUNHA *et al.*, 2008).

Nesse contexto, multiplicam-se os delitos que emergem e se disseminam nesse novo universo, evidenciando a necessidade de regulamentação e controle das atividades no ambiente virtual, uma vez que a internet se configura como tanto o meio quanto o alvo dos agentes criminosos. Delitos já conhecidos, como furto, fraude e estelionato, são perpetrados diariamente na internet de forma explícita (VELLOZO, 2015).

O conceito de violência no ambiente virtual, conforme definido pelo professor Paulo Marco Ferreira Lima, engloba atos de assédio, abuso ou exploração sexual que ocorrem por meio da internet, redes sociais, aplicativos de mensagens e outras plataformas online, denominados por ele como “crimes de computador” (LIMA, 2000).

O fenômeno da violência virtual representa uma das mais severas violações dos direitos humanos, presente não apenas no Brasil, mas globalmente. O direito ao desenvolvimento físico, à vida e à dignidade humana são prerrogativas que proporcionam ao indivíduo a possibilidade de um futuro com plena cidadania e a garantia de outros direitos intrínsecos à vida (LIMA, 2022).

Portanto, o objetivo principal desta pesquisa é analisar os crimes cibernéticos e seu crescimento devido à ausência de legislação eficaz, que se mostra insuficiente na regulamentação das infrações, uma vez que as normas existentes não acompanharam a evolução desses delitos. Os objetivos específicos incluem explicar a conceituação dos crimes cibernéticos, detalhar a evolução desses crimes em contraste com a defasagem normativa, sintetizar suas categorias e características, além de apresentar os desafios relativos à investigação criminal e propor possíveis soluções para o problema em questão.

Assim, este trabalho foi estruturado para tratar o tema de maneira temática, sendo dividido em três partes: inicialmente, aborda o surgimento dos crimes virtuais, com uma exposição do histórico e conceito; em seguida, examina as diferentes espécies de crimes

virtuais; e, finalmente, discute a adaptação do ordenamento jurídico aos delitos típicos da era digital.

A metodologia utilizada neste artigo foi a pesquisa bibliográfica. De natureza científica básica, o estudo visa fornecer conhecimento sobre a temática em questão, adotando uma abordagem qualitativa. Ademais, o método dedutivo é empregado com o propósito de elucidar o conteúdo das ideias, partindo de conceitos gerais para os específicos, com o objetivo de alcançar uma conclusão lógica.

2 SURGIMENTO DE CRIMES VIRTUAIS

Visando aprimorar a rotina e incrementar a eficiência das atividades cotidianas, emergiram os computadores e as redes de comunicação. Tais inovações tecnológicas revolucionaram a forma de trabalhar, comunicar-se e executar uma gama de atividades. Processos que demandavam extenso tempo e esforço manual passaram a ser realizados com agilidade e exatidão.

Desde tempos remotos, a humanidade tem perseguido o desenvolvimento por meio de novos projetos e ferramentas que facilitassem o cotidiano e tornassem as tarefas mais agradáveis. Essa incessante busca por inovação e eficiência é uma constante na trajetória humana, culminando no desenvolvimento de tecnologias que alteraram a sociedade de forma marcante e duradoura (RODRIGUES, 2021).

Nesse percurso, o mundo testemunhou várias transformações significativas, entre as quais se sobressai a Revolução Industrial, um dos eventos mais impactantes. Essa revolução modificou radicalmente o estilo de vida da população, assinalando uma transição do trabalho manual e agrário para a produção industrial e mecanizada. Iniciado na Inglaterra na segunda metade do século XVIII, esse processo se difundiu por outros países, acarretando mudanças substanciais em vários aspectos da sociedade (CARNEIRO, 2018).

O progresso tecnológico durante a Revolução Industrial introduziu uma série de inovações, como a fotografia em 1839, o telefone em 1876 e a luz elétrica em 1879, que alteraram significativamente o modo de vida e a interação social. Essas invenções não só melhoraram a qualidade de vida, mas também abriram novas possibilidades e transformaram a sociedade de formas que perduram até hoje (DIAS, 2004).

Mais adiante, em meados do século XX, ocorreu um marco expressivo no desenvolvimento de novas tecnologias, denominado Era da Informação ou Era Digital, também conhecida como Terceira Revolução Industrial. Esse período foi caracterizado pela

evolução acelerada das tecnologias de informação e comunicação, que transformaram profundamente a sociedade, a economia e a cultura global (DIAS, 2004).

A internet, notavelmente, trouxe incontáveis vantagens e benefícios, interligando relações sociais e comerciais globais em uma rede unificada. Isso propiciou um crescimento econômico exponencial entre nações e alterações significativas na vida cotidiana. A internet permeia diversas atividades diárias, influenciando relações profissionais, financeiras e pessoais (RAMOS; SANTOS, 2022).

Paralelamente às vantagens, a evolução tecnológica no âmbito virtual também originou comportamentos prejudiciais e desafios notáveis. Muitos criminosos perceberam a oportunidade de usar esse espaço virtual como meio para atividades ilícitas. Isso resultou em uma migração significativa de indivíduos com intenções criminosas para o ambiente online, originando uma nova categoria de delitos: os crimes cibernéticos ou virtuais (CASTRO, 2003).

Nesse sentido, afirma Medeiros (2010):

Tal contexto de inovação tecnológica igualmente propiciou o surgimento de novas modalidades de crimes, bem como a expansão de novos métodos de praticar crimes já tipificados na legislação vigente. A partir daí, os conhecimentos tecnológicos inovadores passaram a ser utilizados não apenas para beneficiar a sociedade, mas também se tornaram perigosas ferramentas para a prática de condutas ilícitas e lesivas a diversos bens jurídicos (MEDEIROS, 2010).

O advento do crime virtual está intrinsecamente atrelado ao desenvolvimento e à difusão da internet e das tecnologias digitais. A história dos delitos virtuais tem início com a evolução dos computadores e das redes de comunicação, datando das décadas de 1960 e 1970, período em que os primeiros sistemas computacionais começaram a ser interligados (ARAÚJO, 2023).

Na alvorada da era computacional, os crimes cibernéticos eram escassos, dada a limitada acessibilidade aos computadores. Os incidentes iniciais de invasão de sistemas foram realizados por aficionados por tecnologia e estudantes, movidos pela curiosidade ou pelo desejo de demonstrar competências técnicas. Um dos primeiros registros de invasão ocorreu em 1969, quando discentes da Universidade de Stanford e do MIT infiltraram-se em redes computacionais para testar suas habilidades (CARNEIRO, 2018).

Com a popularização dos computadores pessoais na década de 1980, emergiram os primeiros hackers de renome. O caso de Kevin Mitnick, um dos mais célebres hackers, exemplifica essa era. Mitnick foi capturado por violar sistemas de grandes empresas e subtrair softwares valiosos. Nesse período, o governo estadunidense instituiu a *Computer Fraud and*

Abuse Act (1986), uma das pioneiras legislações a criminalizar práticas de invasão de sistemas (FERREIRA, 2019).

A década de 1990 foi marcada pela proliferação da internet. Com a ascensão da *World Wide Web*, os crimes cibernéticos avançaram em complexidade e quantidade. Novas modalidades de delitos surgiram, como o *phishing*, a propagação de vírus e malwares, além de fraudes eletrônicas. A facilidade de acesso a informações e a comunicação globalizada propiciaram a expansão de atividades ilícitas na rede. Nos anos 2000, os delitos virtuais tornaram-se mais sistematizados e profissionais. Organizações criminosas passaram a enxergar o potencial da internet para a prática de ilícitos em grande escala, como furto de identidade, lavagem de dinheiro, tráfico de entorpecentes e exploração sexual (ARAÚJO, 2023).

O Brasil intensificou a atenção aos crimes cibernéticos especialmente nas últimas décadas, com a popularização da internet e demais inovações tecnológicas. A Constituição Federal de 1988 representou um marco inicial relevante, estabelecendo diretrizes legais para a competência estatal em matéria de informática (BRASIL, 1988).

Em face das incessantes inovações tecnológicas e mudanças socioeconômicas, emergem discussões sobre a Quarta e Quinta Revoluções Industriais. A Quarta Revolução Industrial, ou Indústria 4.0, é caracterizada pela fusão de tecnologias digitais, físicas e biológicas, impulsionada por avanços em inteligência artificial, robótica, Internet das Coisas, computação em nuvem, big data, biotecnologia, nanotecnologia e impressão 3D (STAFF, 2022).

A Quinta Revolução Industrial, ou Indústria 5.0, encontra-se em curso e introduz novos parâmetros de produtividade que transcendem as métricas tradicionais de produção humana e mecânica. Esta revolução é marcada pela colaboração entre humanos e máquinas, enfatizando a personalização, sustentabilidade e ética. A Indústria 5.0 está transformando rapidamente o mundo contemporâneo, acelerada pela pandemia de COVID-19 e pela necessidade de adaptação ágil, promovendo a integração de diferentes espaços e funções, reformulando o modo de viver e trabalhar (FILHO, 2021).

No entanto, à medida que crescem as inovações e possibilidades que beneficiam o estilo de vida, aumentam também os desafios. A hiperconectividade, fruto das revoluções tecnológicas e da integração global, cria um terreno propício para a inovação criminosa e o surgimento de novos agentes desestabilizadores. Diferentemente das revoluções anteriores, a quarta e a quinta se destacam por um ritmo excepcionalmente acelerado, amplitude e

profundidade sem precedentes, impulsionadas pela interconexão de novas tecnologias (FILHO, 2021).

2.1 CONCEITO DE CRIMES VIRTUAIS

Os avanços tecnológicos significativos deram origem aos crimes cibernéticos, que acarretam prejuízos e expõem os usuários da internet, incluindo os de redes sociais como *Instagram, Facebook e Twitter*, entre outras. Esses delitos, perpetrados ou facilitados pelo meio digital, por meio da internet ou de sistemas computacionais, constituem uma ameaça a uma variedade de bens jurídicos, afetando tanto indivíduos quanto patrimônios, sejam eles materiais ou imateriais.

A definição de crimes virtuais diverge conforme a interpretação dos estudiosos. Joseph Migga Kizza caracteriza os crimes virtuais como condutas ilícitas direcionadas contra computadores e redes de computadores, com o intuito de causar danos ou comprometer a integridade dos sistemas de informação (KIZZA, 2005).

Por sua vez, Kunrath esclarece: “Os crimes informáticos são, em sua maioria, delitos comuns praticados com o auxílio de um computador. No entanto, há crimes específicos que ocorrem exclusivamente em sistemas computacionais” (KUNRATH, 2014).

Gouvêa (1997) utiliza a expressão “crimes por meio da informática” para designar delitos que incorporam o uso de tecnologia da informação, sistemas computacionais, redes digitais e dispositivos eletrônicos na execução de atividades ilícitas. A autora justifica sua escolha pela necessidade de enfatizar que os crimes virtuais são infrações intrinsecamente ligadas à tecnologia.

Adicionalmente, Trindade, Albino e Stegmann (2022) afirmam que os crimes cibernéticos são consequência direta do significativo progresso tecnológico, acarretando prejuízos que vulnerabilizam as vítimas, isto é, os usuários da internet, abrangendo várias redes sociais como *Instagram, Facebook e Twitter* (STEGMANN *et al.*, 2022).

Observa-se que, embora os autores abordem o tema sob perspectivas distintas, há um consenso geral de que tais delitos envolvem o emprego de tecnologia digital e computadores. Portanto, a variação reside primordialmente na terminologia empregada para descrever esses crimes.

3 ESPÉCIES DE CRIMES VIRTUAIS

A expansão dos delitos virtuais em redes sociais é potencializada pela ampla divulgação de dados pessoais pelos usuários, pela confiança depositada nas interações sociais e pela velocidade de propagação de informações. Plataformas como Facebook, Instagram e Twitter proporcionam um terreno propício para a ocorrência desses delitos, devido à sua grande base de usuários e à eficiência na disseminação de conteúdo. Neste capítulo, serão examinadas as modalidades mais recorrentes de crimes virtuais e suas dinâmicas contemporâneas (BATISTA, 2022).

3.1 O RACISMO VIRTUAL

O racismo constitui uma prática arraigada, originária de séculos de dominação, exploração e opressão. Historicamente, a noção de superioridade de certas "raças" em detrimento de outras serviu de fundamento para a escravidão, a colonização e variadas formas de discriminação. Apesar dos progressos sociais e jurídicos visando erradicar o racismo, suas manifestações continuam a se fazer presentes em múltiplas facetas, abrangendo desde a discriminação institucionalizada até o racismo do dia a dia e a incitação ao ódio na internet. Frequentemente, as disparidades sociais, econômicas e culturais são instrumentalizadas para perpetuar preconceitos e estereótipos racistas (ALMEIDA, 2019).

A Comissão de Igualdade Racial e Social da OAB/DF reconhece que:

O racismo compreende qualquer ação ou omissão que cause desconforto, constrangimento ofensa à integridade moral, emocional ou psicológica de um indivíduo, ou ainda, que limite o seu acesso a direitos, por pertencer a determinado grupo étnico ou racial politicamente minoritário (OAB/DF, 2023).

A marginalização social e econômica frequentemente conduz à exclusão e ao isolamento de comunidades negras, intensificando a desigualdade e fomentando hostilidade e preconceito. Tal dinâmica se estende ao ambiente virtual, onde manifestações de racismo, tanto sutis quanto explícitas, contribuem para um espaço online nocivo. Crimes virtuais impulsionados por racismo, incluindo discurso de ódio, cyberbullying e ataques virtuais, impactam significativamente a vida das vítimas e espelham padrões discriminatórios da sociedade física (BERLEZE; PEREIRA, 2017).

Conforme mencionado, o fácil acesso e o anonimato oferecidos pelas plataformas digitais frequentemente incentivam a expressão de opiniões negativas e preconceituosas que, de outra forma, poderiam não ser manifestadas no mundo físico. Redes sociais possuem a

capacidade de conectar indivíduos globalmente, permitindo a formação de comunidades virtuais baseadas em interesses comuns, valores compartilhados e, por vezes, preconceitos recíprocos. Tais agrupamentos tendem a reforçar e ampliar preconceitos existentes, criando uma câmara de eco que pode intensificar o discurso de ódio e a discriminação online (BERLEZE; PEREIRA, 2017).

A ausência de moderação efetiva nas plataformas de mídia social pode facilitar a disseminação do discurso de ódio, ao permitir que conteúdos danosos sejam divulgados sem reprimendas. Contudo, é essencial reconhecer que as redes sociais também podem ser instrumentos potentes para fomentar a conscientização e a justiça social, quando utilizadas de maneira responsável e construtiva (FERREIRA, 2019).

O racismo no ambiente virtual pode afetar qualquer indivíduo, independentemente de sua notoriedade ou anonimato. A natureza aberta e democrática da internet possibilita a criação de perfis em redes sociais e a participação em comunidades online, mas também propicia a propagação de discursos de ódio e preconceito racial (FERREIRA, 2019).

3.2 CRIMES CONTRA A INVIOABILIDADE DO PATRIMÔNIO – ESTELIONATO

Conforme estipulado pelo Código Penal brasileiro, em seu artigo 171, o estelionato é caracterizado pela obtenção de vantagem ilícita, para si ou para terceiros, em detrimento de outrem, induzindo ou mantendo alguém em erro por meio de artifício, ardil ou qualquer outro método fraudulento. Nesse âmbito, o estelionatário emprega a internet ou outras tecnologias digitais com o intuito de ludibriar as vítimas e adquirir benefícios ilícitos, tais como dinheiro, informações pessoais ou acesso a contas bancárias (FERREIRA, 2019).

Diversas modalidades de estelionato virtual são praticadas, incluindo fraudes em transações online, nas quais o fraudador cria páginas falsas de comércio eletrônico ou veicula anúncios enganosos para comercializar produtos ou serviços inexistentes ou distintos dos anunciados. Outra prática comum é o roubo de identidade, em que o criminoso obtém acesso a dados pessoais — como números de Seguro Social, datas de nascimento e informações bancárias — para perpetrar fraudes em nome da vítima (CARDOSO, 2017).

Patury destaca que o estelionato figura entre os crimes virtuais de maior relevância no Brasil, ressaltando que o crescimento do comércio eletrônico propiciou um leque ampliado de oportunidades para atividades criminosas, especialmente no que tange à fraude online e ao roubo de identidade (PATURY, 2023).

3.3 VIOLAÇÃO DOS DIREITOS DAS CRIANÇAS E ADOLESCENTES NA INTERNET

A violação dos direitos de crianças e adolescentes na internet representa uma preocupação global em ascensão, à medida que essa população jovem se torna cada vez mais conectada, enfrentando múltiplos perigos no ciberespaço. A exploração sexual, o *cyberbullying* e a exposição a conteúdos impróprios são algumas das maneiras pelas quais seus direitos fundamentais são comprometidos digitalmente. Comumente, pais e responsáveis têm recorrido a meios digitais para proporcionar oportunidades educacionais e de lazer a esse público (RIPAMONTE, 2018).

O ciberespaço permite o anonimato, facilitando a criação de perfis falsificados, conhecidos como "fakes", que podem ser empregados para enganar, manipular ou prejudicar. Esses perfis são frequentemente utilizados por criminosos para ganhar a confiança de crianças e adolescentes e explorá-los, transformando o que deveria ser uma experiência enriquecedora em um risco potencial, especialmente na ausência de proteção e orientação parental (CUSTÓDIO; CABRAL, 2021).

Conforme pesquisa da TIC Kids Online Brasil, realizada pelo Comitê Gestor da Internet no Brasil em 2022, há 22,3 milhões de crianças e adolescentes entre 9 e 17 anos conectados no país, representando 93% dessa faixa etária. Isso sublinha a necessidade de educar e proteger os jovens durante sua navegação no mundo digital (IBDFAM, 2023).

Os principais delitos virtuais contra menores incluem o abuso sexual infantil online, que abrange a produção, distribuição, posse ou intercâmbio de material de abuso pela internet. Perpetradores frequentemente utilizam fóruns, chats ou redes sociais para disseminar tal conteúdo ou contatar vítimas em potencial; o aliciamento para encontros físicos, com adultos atraindo menores para abuso sexual; e o *cyberbullying*, com o uso de tecnologias para intimidar, assediar, ameaçar ou humilhar (CUSTÓDIO; CABRAL, 2021).

Em resumo, o acesso prematuro às redes sociais pode expor crianças e adolescentes a riscos como interações com estranhos e conteúdos inapropriados. A orientação insuficiente e a exposição precoce podem colocá-los em situações vulneráveis, dada a imaturidade para compreender os perigos, como interações com desconhecidos ou divulgação de informações pessoais. Sem supervisão parental adequada, tornam-se suscetíveis a diversos perigos online, enfrentando situações de vulnerabilidade e violência.

4 ADAPTAÇÃO DO SISTEMA JURÍDICO LEGAL AOS CRIMES INERENTES À ERA DIGITAL

No cenário contemporâneo, a crescente dependência de dispositivos eletrônicos e da internet na vida cotidiana tem conduzido a um incremento notável nos delitos virtuais. Um dos desafios prementes para o ordenamento jurídico consiste em acompanhar a velocidade das inovações tecnológicas e das estratégias empregadas por criminosos virtuais. Frequentemente, as legislações vigentes mostram-se inadequadas para abordar novas modalidades de crimes ou são de difícil aplicação devido à natureza global da internet e à complexidade de identificar e processar os infratores (SANTOS; AZEVEDO, 2022).

A globalização impôs transformações significativas à sociedade, demandando adaptações em múltiplos setores, inclusive no âmbito jurídico. Com a expansão dos computadores e da internet, os crimes cibernéticos emergiram como uma preocupação em ascensão, envolvendo atos de extorsão financeira, indução de estresse emocional e danos à reputação. Esses delitos são perpetrados através de dispositivos conectados, e a legislação brasileira necessitou evoluir para enfrentar essas ameaças emergentes e salvaguardar a sociedade (OLIVEIRA, 2011).

O Brasil, a par de outras nações, tem testemunhado um aumento expressivo no número de crimes cibernéticos. Diante dessa realidade, o sistema jurídico brasileiro foi compelido a desenvolver e implementar normativas específicas para tratar desses delitos, visando assegurar a segurança e a proteção dos cidadãos na era digital (SANTOS; AZEVEDO, 2022).

Portanto, é patente que o sistema jurídico brasileiro enfrenta uma miríade de problemas oriundos do advento dos crimes cibernéticos e de sua influência na era digital. A dissolução das fronteiras tradicionais do crime, exacerbada pela globalização, requer uma resposta integrada das forças de segurança e do sistema jurídico em sua totalidade. Contudo, mesmo após avanços legislativos, persistem desafios consideráveis. O desenvolvimento tecnológico acelerado frequentemente ultrapassa a capacidade do sistema jurídico de estabelecer e efetivar regulamentações eficazes, criando um hiato onde delitos virtuais podem ocorrer sem uma resposta legal apropriada e tempestiva (NOGUEIRA; NOLASCO, 2022).

Adicionalmente, conforme Trindade (2022), os delitos digitais tiveram um acréscimo de aproximadamente 260% em 2020 em comparação a 2019. Esse crescimento alarmante é extremamente preocupante, especialmente no tocante à aplicação da lei. A identificação dos agentes de crimes cibernéticos é geralmente complexa, pois estes se beneficiam do anonimato proporcionado pela internet, resultando muitas vezes em impunidade.

A dificuldade em rastrear os perpetradores de crimes cibernéticos é amplamente reconhecida pelos próprios criminosos, incentivando o aumento dessas atividades ilícitas. Tal cenário impõe desafios severos ao sistema jurídico, que necessita não somente de legislação robusta, mas também de técnicas avançadas e cooperação internacional para combater esses crimes de forma efetiva (MARINELI, 2019).

Segundo Cardoso (2017), apesar de as condutas infratoras serem sancionadas, o Código Penal Brasileiro, ainda uma fonte primordial do direito, foi reformulado em 1984, tornando-se menos eficaz no combate às ilegalidades associadas à era digital, visto que a internet ganhou popularidade somente em 1998. Esse descompasso entre a reformulação do Código Penal e o advento da internet apresenta desafios significativos na aplicação da lei aos crimes cibernéticos (CARDOSO, 2017).

O Código Penal, em seu artigo 1º, estabelece: "Não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal". Este princípio, conhecido como legalidade, assegura que ninguém pode ser punido por uma ação que não estava definida como crime pela lei antecedente ao ato. No contexto dos crimes cibernéticos, essa disposição pode suscitar controvérsias, uma vez que muitos dos comportamentos ilícitos atuais não estavam previstos na legislação de 1984 (BRASIL, 1942).

O princípio da legalidade e o princípio da anterioridade da lei penal, com previsão legal no artigo 1º do Código Penal e no artigo 5º, inciso XXXIX, da Constituição Federal de 1988, estipulam que não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal (BRASIL, 1988).

Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: [...]

XXXIX - não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal (BRASIL, 1988).

A ausência de regulamentações específicas para enfrentar os delitos digitais constitui uma falha considerável no sistema jurídico, sobretudo em um contexto de crescente dependência tecnológica. Tal deficiência não somente restringe a capacidade estatal de sancionar os transgressores, mas também promove um clima de impunidade e insegurança social. Internacionalmente, a inércia do Brasil quanto à legislação e prevenção de crimes cibernéticos pode comprometer sua imagem e a eficácia da cooperação com outras nações no combate ao crime digital. A importância dessa colaboração é amplificada pela natureza

transnacional dos delitos cibernéticos, que frequentemente requerem esforços conjuntos para a investigação e processamento dos infratores (SANTOS; AZEVEDO, 2022).

Nesse íterim, a rapidez com que a tecnologia avança muitas vezes excede a capacidade dos legisladores de se manterem atualizados. Como consequência, as normas jurídicas tendem a se tornar obsoletas diante dos novos tipos de criminalidade que emergem no meio digital. Essa discrepância cria um vácuo onde os criminosos podem atuar com certa impunidade, visto que as leis vigentes podem não contemplar especificamente suas condutas (MARINELI, 2019).

Assim, Lopes e Bezerra ressaltam que o direito precisou se adaptar diante da incidência de crimes virtuais e dos desafios jurídicos relacionados à classificação dos crimes cibernéticos, impulsionados pelos avanços tecnológicos no sistema jurídico brasileiro. A elaboração de legislação efetiva e mecanismos de execução da justiça deve ser um processo ágil, capaz de responder adequadamente às modalidades de crime digital que estão em constante transformação. Isso implica que o sistema jurídico do Brasil necessita adotar uma postura proativa, monitorando as inovações técnicas e suas possíveis repercussões no âmbito criminal (LOPES; BEZERRA, 2023).

4.1 CRIMES DIGITAIS E AS LEGISLAÇÕES EXISTENTES

A Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, constitui uma emenda ao Código Penal Brasileiro que aborda especificamente os delitos cibernéticos e informáticos. Essa legislação surgiu como resposta ao aumento de crimes no ambiente virtual, incluindo invasões de dispositivos eletrônicos para apropriação indevida de dados, episódio notório envolvendo a atriz Carolina Dieckmann (BRASIL, 2012).

Sancionada em dezembro de 2012 pela então presidente Dilma Rousseff, após ser proposta em novembro de 2011, a lei marcou um avanço na legislação brasileira ao tipificar de maneira explícita os crimes cibernéticos, prescrevendo penalidades para tais infrações e estabelecendo um arcabouço legal mais robusto para o tratamento de violações de segurança digital (JUSBRAZIL, 2012).

É relevante mencionar que, embora o processo legislativo brasileiro possa ser prolongado, a Lei Carolina Dieckmann constituiu uma exceção, impulsionada pela pressão da mídia e pela urgência decorrente do caso da atriz. A celeridade de sua elaboração e sanção reflete a importância atribuída à segurança digital e a necessidade de atualizar a legislação frente aos desafios do meio virtual. A lei impactou significativamente o Direito Penal do país,

introduzindo dispositivos legais inéditos (artigos 154-A e 154-B) relativos aos crimes cibernéticos e alterando a redação de outros artigos (OLIVEIRA, 2011).

O artigo 154-A, inserido pela Lei Carolina Dieckmann, define o crime de invasão de dispositivo informático, caracterizado pela violação não autorizada de qualquer dispositivo informático de terceiros, como computadores, smartphones e tablets, independentemente de sua conexão com a internet. A lei, portanto, abarca tanto as invasões de dispositivos online quanto offline (OLIVEIRA, 2011).

No que tange à Lei Geral de Proteção de Dados (LGPD), esta se relaciona com os crimes cibernéticos, especialmente no que concerne à proteção de dados pessoais de indivíduos. A LGPD estipula princípios e diretrizes para o processamento de dados pessoais, buscando assegurar a privacidade e a segurança dessas informações. Isso envolve medidas como a exigência de consentimento para o processamento dos dados, a limitação do uso dos dados às finalidades declaradas, a proteção adequada contra acessos não autorizados e a transparência sobre o uso dos dados (SILVA; NOVAIS, 2023).

A LGPD impõe obrigações de segurança aos controladores e operadores de dados, visando a proteção das informações contra acessos indevidos, vazamentos e outras formas de violação. Em situações de crimes cibernéticos associados à violação de dados pessoais, os infratores podem ser responsabilizados conforme as normas da LGPD, o que pode resultar em penalidades severas para organizações que falhem em cumprir as diretrizes de proteção de dados. A lei também estabelece a obrigação de notificar incidentes de segurança que possam afetar a integridade dos dados pessoais, incluindo crimes cibernéticos como violações de segurança e vazamentos de dados (SILVA; NOVAIS, 2023).

Em âmbito jurídico internacional, a Convenção sobre Cibercrimes, realizada em Budapeste em 23 de novembro de 2001 e efetivada em 1º de julho de 2004, visa tipificar os crimes virtuais, abrangendo infrações de sistemas, delitos relacionados ao uso de computadores, crimes envolvendo pedofilia e violações de direitos autorais. A Convenção também trata da competência e cooperação internacional, permitindo que as partes determinem a jurisdição mais adequada para procedimentos legais (KAMINSKI, 2002).

A Convenção de Budapeste busca harmonizar a abordagem aos crimes virtuais e suas formas de persecução penal. O Brasil aderiu à Convenção em 2021, com o propósito de facilitar a cooperação internacional no combate ao cibercrime (CAPEZ, 2012).

Em face do crescimento dos crimes virtuais e do aumento do número de usuários da internet, tanto o Senado Federal quanto a Câmara dos Deputados no Brasil têm alocado recursos para a formulação de legislação sobre crimes cibernéticos. Essa iniciativa reflete a

necessidade de renovar e fortalecer as leis para enfrentar os desafios impostos pela era digital (Reis, 2021).

A evolução acelerada da sociedade demanda uma adaptação contínua do sistema jurídico. Para assegurar a proteção dos direitos em ambientes físicos e digitais, é imprescindível a modernização constante das leis e a atuação efetiva do Estado. Assim, o sistema jurídico pode manter sua relevância e eficácia na promoção da justiça e na salvaguarda dos direitos no contexto de uma sociedade digital em constante mudança (REIS, 2021).

A Convenção de Budapeste, também conhecida como Convenção sobre o Cibercrime, é um marco na legislação internacional sobre crimes virtuais. Instituída pelo Conselho da Europa na Hungria em 2001, a convenção entrou em vigor em 2004, após ratificação por cinco países, e tem sido adotada progressivamente por um número crescente de Estados-membros e alguns não membros (MANGO, 2023).

A Convenção de Budapeste é estruturada em quatro capítulos que delineiam os aspectos cruciais do combate aos crimes cibernéticos: definições e terminologia (Capítulo I); medidas nacionais (Capítulo II); cooperação internacional (Capítulo III); e cláusulas finais (Capítulo IV). As definições de crimes cibernéticos são extensivas, abarcando uma gama de atividades ilícitas, tais como violação da confidencialidade de sistemas e dados, infração de direitos autorais, acesso não autorizado a sistemas e interceptação ilegal de comunicações. O propósito central da Convenção é a identificação e tipificação de delitos cometidos na internet, estabelecendo um marco legal uniforme para o tratamento de questões de cibersegurança, como invasões de sistemas (*hacking*), fraudes eletrônicas, pornografia infantil, dentre outros crimes virtuais (MANGO, 2023).

Adicionalmente, a Convenção foi ratificada por vários Estados não membros do Conselho da Europa, incluindo Argentina, Canadá, Chile, Colômbia, Estados Unidos, República Dominicana e Peru, evidenciando o reconhecimento global da importância da cooperação internacional no enfrentamento dos crimes cibernéticos e a necessidade de um arcabouço legal abrangente para superar esses desafios (LIMA, 2000).

No contexto brasileiro, existem iniciativas legislativas voltadas para a tecnologia e crimes virtuais. No entanto, a legislação atual é frequentemente considerada insuficiente para endereçar os desafios emergentes, visto que muitos projetos de lei pertinentes permanecem em tramitação no Congresso Nacional por períodos extensos, retardando a implementação de medidas legislativas essenciais para a resolução de problemas relacionados à temática (RAMOS; SANTOS, 2022).

Embora haja desafios na legislação específica para delitos informáticos, isso não implica a ausência de regulamentação no Brasil para lidar com tais questões. De fato, diversas condutas criminosas associadas à tecnologia podem ser subsumidas sob tipos penais existentes na legislação nacional, como o Código Penal. Exemplos incluem invasão de sistemas, interceptação ilegal de comunicações, falsificação de documentos eletrônicos e fraude eletrônica, que podem ser considerados crimes conforme as disposições vigentes no Código Penal Brasileiro (LIMA, 2000).

Portanto, mesmo na falta de legislação específica para crimes cibernéticos, os infratores podem ser responsabilizados e julgados com base no ordenamento jurídico preexistente no Brasil, desde que as condutas delitivas se enquadrem nos tipos penais definidos.

5 CONSIDERAÇÕES FINAIS

A ausência de legislação específica pode obstar a investigação e sanção de delitos perpetrados via internet. No Brasil, embora existam dispositivos legais aplicáveis, tais como o Código Penal e o Marco Civil da Internet, a inexistência de normas específicas pode acarretar lacunas e desafios na efetivação da justiça.

A carência de normativas direcionadas aos crimes cibernéticos pode acarretar insegurança jurídica para cidadãos e para o sistema de justiça. Legislações mal elaboradas ou precipitadas, a exemplo da Lei nº 12.737/2012, podem gerar consequências adversas, como imprecisão na tipificação dos delitos e na cominação de penalidades adequadas.

Destaca-se, portanto, que a elaboração de legislação concernente a crimes virtuais demanda uma abordagem metódica e ponderada. Considerando a evolução célere do ciberespaço e das tecnologias digitais, é imperativo que qualquer normativa seja redigida de maneira apropriada e suficientemente flexível para enfrentar desafios e contextos emergentes.

Não obstante a importância vital de legislações específicas para regular delitos no meio virtual, estas não se mostram suficientes. Existem outras estratégias complementares essenciais para o enfrentamento dos crescentes desafios digitais.

É primordial fomentar programas de conscientização e educação tecnológica para a população, enfocando temas como segurança digital, proteção de dados pessoais e identificação de ameaças virtuais. Tais iniciativas podem ser implementadas por meio de campanhas midiáticas, currículos escolares atualizados e capacitações para adultos. Ademais, é crucial oferecer treinamento especializado em segurança cibernética e investigação de

delitos digitais a agentes estatais, incluindo policiais, promotores e magistrados, habilitando-os a enfrentar os desafios técnicos e jurídicos atrelados aos cibercrimes. Igualmente importante é estabelecer parcerias e acordos internacionais para o intercâmbio de informações e práticas eficazes no combate a esses delitos, que frequentemente ultrapassam fronteiras nacionais e requerem cooperação transnacional.

Diante do exposto, evidencia-se a necessidade de integrar a instituição de legislação específica para reprimir condutas ilícitas virtuais à implementação de políticas públicas que incentivem a educação tecnológica e capacitação de agentes públicos, sendo estas fundamentais para uma atuação efetiva frente aos desafios do ambiente digital em constante expansão.

REFERÊNCIAS

- ANGO, Carolina Mattioli Martino. **Efeitos da convenção de Budapeste nas relações jurídicas nacionais**. 2023. Disponível em: <<https://www.migalhas.com.br/depeso/388700/efeitos-da-convencao-de-budapeste-nas-relacoes-juridicas-nacionais>>. Acesso em: 10 abr. 2024.
- ARAÚJO, Cláudio Rodrigues. **Crimes Virtuais**. Belo Horizonte: Editora Expert, 2023.
- BATISTA, Lorena Prado. **Crimes cibernéticos: uma análise sobre como a tecnologia está a serviço da criminalidade no Brasil**. Goiânia, 2022. Disponível em: <<https://repositorio.pucgoias.edu.br/jspui/bitstream/123456789/4706/1/Trabalho%20LORENA%20Prado.pdf>>. Acesso em: 20 maio 2024.
- BERLEZE, Michele; PEREIRA, Berlinda Silva. **O racismo nas redes sociais: o preconceito real assumido na vida virtual**. 201. Disponível em: <<https://www.ufsm.br/app/uploads/sites/563/2019/09/1-6-2.pdf>>. Acesso em: 05 maio 2024.
- CAPEZ, Fernando. **Curso de direito penal: parte especial: arts. 121 a 212**. São Paulo: Editora Saraiva, 2019. v. 2. ISBN 9788553609444.
- CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática e seus Aspectos Processuais**. 2. ed. Rio de Janeiro: Lumen Juris, 2003.
- CATAPAN, Edilson Antonio. **Estudos sobre funcionamento, desenvolvimento e organização das sociedades**. São José dos Pinhais: Editora Brazilian Journals, 2021.
- BRASIL. **Código penal**. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acesso em: 16 out. 2023.
- CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. São Paulo: Saraiva, 2011.
- CUNHA, E. P.; SILVA, E. M.; GIOVANETTI, A. C. **Enfrentamento à violência sexual infante-juvenil: expansão do PAIR em Minas Gerais**. Belo Horizonte: UFMG, 2008.

CUNHA, Rogério Sanches. **Manual de Direito Penal: Parte Geral**. Salvador: Juspodivm, 2014.

CUSTÓDIO, André Viana; CABRAL, Johana. **A violação de direitos de crianças e adolescentes por assédio moral nos ambientes sociais e virtuais**. Revista Meritum, v. 16, 2021.

FERREIRA, Ivette Senise. **A criminalidade informática**. In: LUCCA, Newton de; SIMÃO FILHO, Adalberto (Coord.). **Direito & Internet: Aspectos Jurídicos Relevantes**.

FILHO, Paulo Roberto Aguiar de Lima. **O direito penal na quarta revolução industrial: a expansão razoável frente aos crimes cibernéticos**. Delictae, vol. 6, 2021. Disponível em: <<https://delictae.com.br/index.php/revista/article/view/150/115>>. Acesso em: 18 maio 202.

FONSECA, J. J. S. **Metodologia da Pesquisa Científica**. Fortaleza: UEC, 2002. Apostila.

GOUVÊA, Sandra. **O direito na era digital: crimes praticados por meio da informática**. Rio de Janeiro: Mauad Editora Ltda, 1997.

IBDFAM. **Sharenting: especialistas avaliam os riscos da exposição infantil nas redes sociais**. 2023. Disponível em: <<https://ibdfam.org.br/noticias/11416/Sharenting%3A+especialistas+avaliam+os+riscos+da+exposi%C3%A7%C3%A3o+infantil+nas+redes+sociais>>. Acesso em: 12 abr. 2024.

JESUS, Damásio Evangelista de. **Manual de Crimes Informáticos**. 1ª ed. São Paulo: Saraiva, 2016.

KIZZA, Joseph Migga. **Computer Network Security**. 2005.

LIMA, Gisele Truzzi de. **Redes Sociais e Segurança da Informação**. Disponível em: <<https://truzzi.com.br/pdf/artigo-redes-sociais-e-seguranca-da-informacao.pdf>>. Acesso em: 10 out. 2023.

LIMA, Jessica; AZEVEDO, Delner do Carmo. **Crimes cibernéticos no Brasil**. Revista Científica Semana Acadêmica. Fortaleza, 2022. Disponível em: <<https://semanaacademica.org.br/artigo/crimes-ciberneticos-no-brasil>>. Acesso em: 08 maio 2024.

NETO, Côrtes; DE LIMA, Honorio. **Exploração sexual infantil pela internet: princípios gerais para construção de uma política pública de enfrentamento**. 2022.

NOGUEIRA, Sandro D'Amara. **Crimes de Informática**. Leme: BH Editora, 2009.

OLIVEIRA, Gilberto Gonçalves de. **Pesquisa em Conteúdo jurídico, Crimes Cibernéticos**. 2011. Disponível em: <<https://conteudojuridico.com.br/consulta/Artigos/52512/crimes-ciberneticos>>. Acesso em: 27 mar. 2024.

OTSU, Denise Pereira. **Crimes digitais e os limites da liberdade expressão nas redes**. São Paulo-SP, 2023.

PAESANI, Liliana Minardi. **Direito e Internet: liberdade de informação, privacidade e responsabilidade civil.** Disponível em:

<<http://repositorio.aee.edu.br/bitstream/aee/18227/1/Gabrielly%20Daianne.pdf>>. Acesso em: 08 mar. 2024.

PATURY, Fabrício Rabelo. **A Política Criminal do Núcleo de Combate aos Crimes Cibernéticos do Ministério Público do Estado da Bahia no enfrentamento aos ilícitos cometidos no âmbito digital.** MPBA. Disponível em:

<https://www.mpba.mp.br/sites/default/files/biblioteca/criminal/artigos/diversos/a_politica_criminal_do_nucleo_de_combate aos_crimes_ciberneticos_do_ministerio_publico_do_estado_da_bahia_-_fabricio_rabelo_patury_e_fernanda_veloso_salgado.pdf>. Acesso em: 13 mai. 2024.

PINHEIRO, Patrícia Peck. **Direito Digital.** 4. ed. São Paulo: Saraiva, 2010.

PRODANOV, C. C.; FREITAS, E. C. **Metodologia do Trabalho Científico: Métodos e Técnica da Pesquisa e do Trabalho Acadêmico.** 2. ed. Novo Hamburgo: Feevale, 2013.

RAMOS, Alicia Castro; SANTOS, Jackson Novaes. **A fragilidade do ordenamento jurídico quanto ao cibercrime: criminosos por trás de uma tela, vítimas expostas em suas vidas reais.** *Revista Ibero-Americana de Humanidades, Ciências e Educação- REASE.* São Paulo, v.8, 2022.

REIS, Caio Gonçalves. **Crimes virtuais: Uma análise acerca da (in) eficácia da legislação e os desafios de sua persecução penal.** 2021. Disponível em:

<<https://www.jusbrasil.com.br/artigos/crimes-virtuais-uma-analise-acerca-da-in-eficacia-da-legislacao-e-os-desafios-de-sua-persecucao-penal/1220973039>>. Acesso em: 20 abr. 2024.

RIPAMONTE, Rafael Henrique. **Violência Contra Crianças e Adolescentes na Internet.** JUSBRASIL, 2018. Disponível em: <<https://www.jusbrasil.com.br/artigos/violencia-contra-criancas-e-adolescentes-na-internet/654833090>>. Acesso em: 15 mai. 2024.

RODRIGUES, Nathana Alves. **Ciber Crimes: Os Desafios Na Atual Legislação Brasileira.** Disponível em: <<https://jus.com.br/artigos/93970/ciber-crimes-os-desafios-na-atual-legislacao-brasileira>>. Acesso em: 25 mai. 2024.

SAMPAIO, R. F.; MANCINI, M. C. **Estudos de Revisão Sistemática: Um Guia Para Síntese Criteriosa da Evidência Científica.** *Rev. bras. Fisioter.* 2007. p. 83-89.

SILVA, Ronaldo Couto da; NOVAIS, Thyara Gonçalves. **A LEI GERAL DE PROTEÇÃO DE DADOS E SUA APLICAÇÃO NO COMBATE AOS CRIMES CIBERNÉTICOS: DESAFIOS E PERSPECTIVAS.** *Ver. Ibero-Americana de Humanidades, Ciências e Educação- REASE.* 2023.

STAFF, SONICWALL. **Segurança Cibernética na Quinta Revolução Industrial.**

Disponível em: <<https://blog.sonicwall.com/pt-br/2022/05/seguranca-cibernetica-na-quinta-revolucao-industrial/>>. Acesso em: 15 mai. 2024.

SYDOW, Spencer Toth. **Delitos informáticos próprios: uma abordagem sob a perspectiva vitimodogmática**. Universidade de São Paulo, São Paulo, 2009. Disponível em: <https://egov.ufsc.br/portal/sites/default/files/delitos_informaticos_proprios_uma_abordagem_sob_a_perspectiva_vitimodogmatica.pdf>. Acesso em: 02 out. 2023.

TRINDADE, Hairton Yoshiaki Hidaka; ALBINO, Matheus de Oliveira Marques; STEGMANN, Vinícius Umbelino. **Crimes cibernéticos: a fragilidade no ordenamento jurídico brasileiro**. CIENCIAS JURÍDICAS. v.26, 2022.

VELLOZO, Jean Pablo Barbosa. **Crimes informáticos e criminalidade contemporânea**. 2015. Disponível em: <<https://jus.com.br/artigos/44400/crimes-informaticos-e-criminalidade-contemporanea>>. Acesso em: 15 set. 2023.

PARECER DE REVISÃO ORTOGRÁFICA/GRAMATICAL E NORMATIVA ABNT

Eu, Aline Rodrigues Ferreira, graduada em Biblioteconomia pela Universidade Federal do Cariri, atesto que realizei a revisão ortográfica e gramatical do trabalho intitulado **“CRIMES NA ERA DIGITAL: Análise da Fragilidade do Ordenamento Jurídico em Relação aos Crimes Praticados em Ambiente Virtual”**, de autoria de Karen Santos de Oliveira, sob orientação do (a) Francisco Thiago da Silva Mendes. Declaro que este TCC está em conformidade com as normas da ABNT e apto para ser submetido à avaliação da banca examinadora de Trabalho de Conclusão de Curso do Centro Universitário Doutor Leão Sampaio/UNILEÃO.

Documento assinado digitalmente
 **ALINE RODRIGUES FERREIRA**
Data: 10/06/2024 22:11:49-0300
Verifique em <https://validar.iti.gov.br>

Juazeiro do Norte, 10/06/2024

ALINE RODRIGUES FERREIRA

PARECER DE TRADUÇÃO DO RESUMO PARA LINGUA INGLESA

Eu, José Alex Ferreira Rodrigues, com formação no curso de Inglês avançado, pelo Instituto Federal do Rio Grande do Sul (IFRS), atesto que realizei a tradução do resumo do trabalho intitulado **“CRIMES NA ERA DIGITAL: Análise da Fragilidade do Ordenamento Jurídico em Relação aos Crimes Praticados em Ambiente Virtual”**, de autoria de KAREN SANTOS DE OLIVEIRA, sob orientação do Prof. Me. Francisco Thiago da Silva Mendes. Declaro que o ABSTRACT inserido neste TCC está apto à entrega e análise da banca avaliadora de Trabalho de Conclusão de Curso do Centro Universitário Doutor Leão Sampaio/Unileão.

Juazeiro do Norte, 10/06/2024



Documento assinado digitalmente

JOSE ALEX FERREIRA RODRIGUES

Data: 10/06/2024 22:49:50-0300

Verifique em <https://validar.iti.gov.br>

JOSE ALEX FERREIRA RODRIGUES