CENTRO UNIVERSITÁRIO FAEMA – UNIFAEMA

THAÍS GIEGA DE SOUZA

CRIMES CIBERNÉTICOS X DIREITOS HUMANOS: OS DESAFIOS DA INVESTIGAÇÃO FORENSE E OS EFEITOS PSICOLÓGICOS ENFRENTADOS NA SOCIEDADE CONTEMPORÂNEA NO MUNDO DIGITAL

ARIQUEMES/RO

2025

THAÍS GIEGA DE SOUZA

CRIMES CIBERNÉTICOS X DIREITOS HUMANOS: OS DESAFIOS DA INVESTIGAÇÃO FORENSE E OS EFEITOS PSICOLÓGICOS ENFRENTADOS NA SOCIEDADE CONTEMPORÂNEA NO MUNDO DIGITAL

Artigo científico apresentado ao Centro Universitário FAEMA (UNIFAEMA), como requisito parcial para a obtenção do título de Bacharela em Direito.

Orientador (a): Prof.ª Esp. Maria Eduarda Ribeiro da Silva.

ARIQUEMES/RO

2025

Dados Internacionais de Catalogação na Publicação

Centro Universitário Faema - UNIFAEMA

Gerada mediante informações fornecidas pelo(a) Autor(a)

S729c SOUZA, Thaís Giega de

Crimes cibernéticos x direitos humanos: os desafios da investigação forense e os efeitos psicológicos enfrentados na sociedade contemporânea no mundo digital/ Thaís Giega de Souza – Ariquemes/ RO, 2025.

38 f.

Orientador(a): Profa. Esp. Maria Eduarda Ribeiro da Silva

Trabalho de Conclusão de Curso (Bacharelado em Direito) – Centro Universitário Faema - UNIFAEMA

1.Crimes cibernéticos. 2.Digital investigação forense. 3.Justiça. I.Silva, Maria Eduarda Ribeiro de.. II.Título.

CDD 340

Bibliotecário(a) Poliane de Azevedo CRB 11/1161

THAÍS GIEGA DE SOUZA

CRIMES CIBERNÉTICOS X DIREITOS HUMANOS: OS DESAFIOS DA INVESTIGAÇÃO FORENSE E OS EFEITOS PSICOLÓGICOS ENFRENTADOS NA SOCIEDADE CONTEMPORÂNEA NO MUNDO DIGITAL

Artigo científico apresentado ao Centro Universitário FAEMA (UNIFAEMA), como requisito parcial para a obtenção do título de Bacharela em Direito.

Orientadora: Prof.ª Esp. Maria Eduarda Ribeiro da Silva.

BANCA EXAMINADORA

Documento assinado digitalmente
gov.br
MARIA EDUARDA RIBEIRO DA SILVA
Data: 06/12/2025 19:02:48-0300
Verifique em https://validar.iti.gov.br

Prof.ª Esp. Maria Eduarda Ribeiro da Silva - orientadora
Centro Universitário FAEMA – UNIFAEMA

Assinado digitalmente por: Rubens Darolt Junior
Razão: Sou responsável pelo documento
Localização: UNIFAEMA - Ariquemes/RO
O tempo: 03-12-2025 17:13:34

Prof. Esp. Rubens Darolt Júnior - examinador
Centro Universitário FAEMA – UNIFAEMA

PAULO ROBERTO MELONI MONTEIRO
Assinado digitalmente por PAULO ROBERTO MELONI MONTEIRO
ND: C=BR, S=Rondonia, L=Ariquemes, O=Centro Universitario Faema - UNIFAEMA, CN=PAULO ROBERTO MELONI MONTEIRO, OU=PAULO ROBERTO MELONI MONTEIRO
Razão: Eu sou o autor deste documento
Localização:
Data: 2025.12.05 18:34:02-04'00'
Foxit PDF Reader Versão: 2025.1.0

Prof. Esp. Paulo Roberto Meloni Monteiro - examinador
Centro Universitário FAEMA - UNIFAEMA

ARIQUEMES/RO

2025

Dedico este lindo trabalho ao meu lindo Deus, aos meus amados pais, aos meus irmãos, ao meu precioso futuro esposo, a minha Mel, aos meus avós, familiares e amigos, que me apoiaram e incentivaram a seguir em frente nesta belíssima e árdua aventura acadêmica.

AGRADECIMENTOS

Primeiramente, agradeço à Trindade — ao Pai, ao Filho e ao Espírito Santo — por ter me ouvido através das minhas orações genuínas antes mesmo de cursar Direito, e Ele me escutou e realizou o tão sonhado desejo do meu pequeno coração, me concedeu a força que vem do céu, em cada experiência vivida ao longo deste curso, em cada alegria e cada lágrima, meu Deus esteve presente, mostrando quem Ele é em minha vida, o grande EU SOU. Não me deixou sozinha; Ele é e sempre será o maior motivo de eu estar aqui firme e forte. Foi Ele quem mais acreditou em mim, no meu potencial, e sempre estivemos juntos em tudo — nos estudos, nos trabalhos, nas apresentações, nas provas, nas atividades, do mais simples ao mais complexo. Tudo fizemos juntos, e irei honrá-Lo através desta graduação e da minha profissão. Obrigada demais, Deus, Jesus e Espírito Santo, amo-lhes sempre.

Agradeço a minha pessoa, pois mesmo diante de todas as dificuldades que enfrentei, mantive firmeza, determinação, fé, força e paciência. Busquei fazer o meu melhor em tudo que coloquei as minhas mãos. Com minha fé em Deus e cafezinho vi possibilidades no impossível.

Aos meus pais, Carlos e Nicéia, que sempre foram meus maiores incentivadores e investiram tanto em mim. Foram eles que mais estiveram comigo nessa caminhada — nos dias bons e nos dias ruins — sempre presentes, me alertando, orientando e aconselhando com amor e sabedoria. Foram meu braço direito em todos os momentos, a base que me sustentou quando pensei em desistir e a voz que me encorajou a continuar. Agradeço grandemente a Deus pela vida dos dois, por tudo o que representam e por todo o amor, puxão de orelha e apoio, pois, juntos fomos mais fortes do que qualquer tempestade. Amo demais vocês.

Aos meus irmãos, Pedro Miguel e Tamily, que são verdadeiros alicerces na minha vida, cada um, com o seu jeito único, me ajudou a ser quem sou e me inspira todos os dias a buscar ser alguém melhor. Agradeço ao Senhor pela vida dos dois, por todo o amor, incentivo, sorrisos, e presença que me fortaleceram ao longo desta caminhada. Pensei neles muitas vezes durante os processos do curso, e o amor genuíno que sinto por eles foi uma das minhas maiores motivações para seguir firme até o fim. Amo vocês, meus docinhos.

Ao meu futuro precioso esposo, Diego Antonio, que me apoia em cada decisão, me motiva, me corrige quando necessário, me espera em tudo, e me eleva sempre. O seu amor verdadeiro é fundamento que me manteve firme, impulsionou-me a seguir em frente e nunca permitiu que eu desistisse — um verdadeiro presentão de Deus na minha vida. Amo-te.

Minha gratidão, à minha Mel, minha fiel companheira desde o ensino fundamental até hoje, que esteve ao meu lado em todo o processo da faculdade, em cada trabalho, em cada estudo, em cada dificuldade, sempre me acompanhava sem falar sequer uma palavra, mas a presença dela foi crucial e tão importante que só Deus sabe, ela sempre foi minha maior companheira.

Agradeço também à minha avó Belarmina, que, mesmo não estando mais aqui, me incentivou a manter o esforço pelos estudos e dedicação com força e honra, ela me mostrou o valor que tem de eu ser uma mulher/moça de princípios; à minha avó Terezinha, que sempre orou por mim e esteve presente, com tanto amor e coração. Aos meus avôs. À minha amiga e conselheira Ivoneti, pela presença constante, pelo apoio generoso, e por estar ao meu lado em tantos momentos, iluminando meu caminho tanto na jornada acadêmica quanto na vida, você é uma joia na minha vida.

Meus agradecimentos vão também à orientadora Maria Eduarda, que acolheu grandemente o tema que tanto desejava em desenvolver, permitindo que eu o mantivesse até o fim. Suas orientações e imensa paciência foram essenciais para que eu chegasse até aqui. Minha sincera gratidão.

Agradeço aos docentes Examinadores por aceitarem o convite para compor a minha banca, pela disponibilidade e generosidade em contribuir com o meu trabalho de pesquisa e com a conclusão desta jornada.

Agradeço ao Unifaema, pela grande oportunidade. Enfim, a todos os amigos e àqueles que contribuíram direta ou indiretamente para a realização desse tão sonhado sonho de uma menina que tinha apenas seus 12 anos de idade.

“Porque eu, o Senhor, amo a justiça e odeio o roubo e toda injustiça.
Em minha fidelidade os recompensarei e com eles farei aliança eterna”.
(Isaías 61:8)

“Gastar mais com café do que com segurança cibernética? Você está pedindo para ser hackeado”. (Richard Clarke)

SUMÁRIO

CRIMES CIBERNÉTICOS X DIREITOS HUMANOS: OS DESAFIOS DA INVESTIGAÇÃO FORENSE E OS EFEITOS PSICOLÓGICOS ENFRENTADOS NA SOCIEDADE CONTEMPORÂNEA NO MUNDO DIGITAL

CYBERCRIMES AND HUMAN RIGHTS: THE CHALLENGES OF FORENSIC INVESTIGATION AND THE PSYCHOLOGICAL EFFECTS FACED IN CONTEMPORARY SOCIETY IN THE DIGITAL WORLD

Thaís Giega de Souza[1]
Maria Eduarda Ribeiro da Silva[2]

RESUMO

Com o avanço da Internet e sua ampla disseminação na sociedade contemporânea, surgiram inúmeras oportunidades e desafios no mundo digital. Entre os benefícios, destaca-se o acesso rápido à informação e a facilidade de comunicação global. Contudo, em contrapartida, emergem ameaças cada vez mais complexas, como o crescimento dos crimes cibernéticos, que têm impactado profundamente a vida de indivíduos, empresas e instituições. Conforme Andrade (2024), o aumento dessas práticas ilícitas exige respostas técnicas e jurídicas mais eficazes, sobretudo diante da lentidão do sistema judiciário e da carência de especialização em cibersegurança e tecnologia. A investigação forense digital tem se mostrado uma ferramenta essencial na identificação e responsabilização de autores de delitos virtuais. Por meio dela, é possível coletar, analisar e apresentar evidências digitais extraídas de dispositivos, redes sociais e plataformas de comunicação. Esse trabalho técnico permite apurar crimes como fraudes, estelionatos, cyberbullyings, stalkings, crimes contra a honra, pornografia infantil, extorsão, disseminação de malwares entre tantos outros. Assim, a perícia digital atua como um elo fundamental entre a tecnologia e a justiça, garantindo a preservação da integridade das provas e o rastreamento de criminosos. Apesar de sua relevância, o campo forense digital ainda enfrenta inúmeros desafios no Brasil, entre eles a insuficiência de peritos especializados, a falta de investimentos públicos e privados e a ausência de infraestrutura tecnológica compatível com a complexidade dos crimes virtuais enfrentados dia após dia. Nesse sentido, especialmente no tocante ao estudo de cyber inteligência, compreendendo que, na atualidade, os crimes no mundo digital têm disparado exacerbadamente. A rápida evolução das ameaças digitais exige constante atualização técnica e compromisso ético dos profissionais, que devem atuar com precisão, empatia e senso de justiça para assegurar a eficácia das investigações, afinal, quanto mais se expandem as informações e o uso das mídias sociais, maior se torna a propagação desses atos delituosos no berço digital. Além das consequências materiais e jurídicas, os efeitos psicológicos decorrentes dos crimes cibernéticos têm sido alarmantes. As vítimas, frequentemente, sofrem humilhação pública, exposição indevida, perseguição e intenso sofrimento

1 Graduanda em Direito pelo Centro Universitário FAEMA – UNIFAEMA. E-mail: thais.36784@unifaema.edu.br.

2 Professora do Centro Universitário FAEMA – UNIFAEMA e Advogada especialista em Direito. E-mail: maria.eduarda@unifaema.edu.br.

emocional. Tais práticas violam diretamente direitos fundamentais assegurados pela Constituição Federal, como a intimidade, a honra e a dignidade da pessoa humana. O impacto emocional dessas agressões digitais pode gerar traumas duradouros, ansiedade e depressão, tornando urgente a implementação de políticas públicas voltadas à prevenção e ao acolhimento das vítimas. Dessa forma, este estudo tem como objetivo analisar a importância da investigação forense no combate aos crimes cibernéticos, identificando os principais delitos praticados, os obstáculos enfrentados pela perícia e a necessidade de valorização e capacitação de profissionais qualificados. A pesquisa, de caráter descritivo, bibliográfico e dedutivo, fundamenta-se em doutrinas, artigos científicos e legislações pertinentes à cibercriminalidade e à atuação pericial. Conclui-se que o perito forense digital exerce papel essencial na proteção dos direitos humanos no ciberespaço, sendo indispensável à efetividade da justiça e à reconstrução da segurança e da integridade da sociedade como um todo.

Palavras-chave: crimes cibernéticos; digital investigação forense; justiça.

ABSTRACT

With the advancement of the Internet and its widespread dissemination in contemporary society, countless opportunities and challenges have arisen in the digital world. Among the benefits are rapid access to information and ease of global communication. However, on the other hand, increasingly complex threats are emerging, such as the growth of cybercrime, which has profoundly impacted the lives of individuals, companies, and institutions. According to Andrade (2024), the increase in these illegal practices requires more effective technical and legal responses, especially given the slowness of the judicial system and the lack of expertise in cybersecurity and technology. Digital forensic investigation has proven to be an essential tool in identifying and holding perpetrators of cybercrimes accountable. Through it, it is possible to collect, analyze, and present digital evidence extracted from devices, social networks, and communication platforms. This technical work allows for the investigation of crimes such as fraud, embezzlement, cyberbullying, stalking, crimes against honor, child pornography, extortion, and the spread of malware, among many others. Thus, digital forensics acts as a fundamental link between technology and justice, ensuring the preservation of evidence integrity and the tracking of criminals. Despite its relevance, the field of digital forensics still faces numerous challenges in Brazil, including a shortage of specialized experts, a lack of public and private investment, and the absence of technological infrastructure compatible with the complexity of the cybercrimes faced on a daily basis. In this sense, especially with regard to the study of cyber intelligence, it is important to understand that crimes in the digital world have skyrocketed in recent years. The rapid evolution of digital threats requires constant technical updating and ethical commitment from professionals, who must act with precision, empathy, and a sense of justice to ensure the effectiveness of investigations. After all, the more information and the use of social media expand, the greater the spread of these criminal acts in the digital realm. In addition to the material and legal consequences, the psychological effects of cybercrimes have been alarming. Victims often suffer public humiliation, undue exposure, persecution, and intense emotional distress. Such practices directly violate fundamental rights guaranteed by the Federal Constitution, such as privacy, honor, and human dignity. The emotional impact of these digital attacks can cause lasting trauma, anxiety, and depression, making it urgent to implement public policies aimed at prevention and victim support. Thus, this study aims to analyze the importance of forensic investigation in combating cybercrimes, identifying the main crimes committed, the obstacles faced by forensic experts, and the need to value and train qualified professionals. The research, which is descriptive, bibliographic, and deductive in nature, is based on doctrines, scientific articles, and legislation relevant to cybercrime and forensic work. It concludes

that digital forensic experts play an essential role in protecting human rights in cyberspace, being indispensable to the effectiveness of justice and the reconstruction of security and integrity in society as a whole.

Keywords Digital; cybercrime; forensic investigation; justice.

1 INTRODUÇÃO

Com a ampla difusão da *Internet* e a crescente transformação das relações sociais, surgem não apenas oportunidades inéditas de comunicação e acesso à informação, mas também desafios complexos no meio digital. Entre eles, destacam-se os crimes cibernéticos, cuja incidência tem se intensificado, afetando diretamente indivíduos, empresas e instituições e exigindo respostas cada vez mais especializadas e eficientes. No tocante a isso, os crimes tipificados por invasão de dispositivo informático como: fraudes (furto/roubo de identidade), estelionatos, *cyberbullying, stalking*, crimes contra a honra, pornografia infantil, e disseminação de *malwares (ransomware)* são apenas algumas das práticas ilícitas que têm demandado diariamente a necessidade da eficaz investigação forense digital no Brasil e mundo, que é uma ferramenta essencial para a coleta, análise e preservação de evidências, garantindo que a justiça possa responsabilizar os verdadeiros autores desses delitos.

No tocante, segundo Cadilhac (2022), a perícia digital no Brasil tem um papel mais que crucial, porém enfrenta diversos desafios, como a carência de profissionais qualificados, insuficiência de investimentos e limitações tecnológicas, agravados pela complexidade crescente das ameaças digitais. Paralelamente, o impacto psicológico sobre as vítimas, que muitas vezes sofrem exposição indevida, perseguição e traumas emocionais duradouros, evidencia a necessidade urgente de políticas públicas de prevenção e acolhimento.

Diante desse panorama, torna-se imperativa a valorização da investigação forense digital, aliadas às tecnologias, conscientização social e à capacitação técnica de profissionais. Somente com a integração entre conhecimento, ética e inovação será possível minimizar a incidência dos delitos virtuais, assegurando um ambiente digital mais seguro, responsável e humanizado, capaz de proteger tanto os indivíduos quanto a sociedade como um todo. O escopo principal deste artigo é demonstrar de forma objetiva a necessidade de elaboração de uma legislação penal e processual específicas, a fim de tomar mais efetivo o combate ao crime cibernético.

2 A EVOLUÇÃO DIGITAL

A rede global de computadores surgiu a partir de um audacioso projeto militar dos Estados Unidos, desenvolvido na década de 1960 pela Agência de Projetos de Pesquisa Avançada do Departamento de Defesa norte-americano (DARPA), cujo propósito era resguardar as comunicações do país diante de uma possível ofensiva soviética. No ápice da Guerra Fria, já se reconhecia a existência de um novo recurso estratégico a ser protegido: os bens informacionais.

Na visão de Lima (2024, p. 11):

> após a revolução tecnológica e digital advinda, sobretudo, da eclosão da *Internet*, o modo de comunicação se transformou demasiadamente, gerando interações cada vez mais instantâneas e globais, onde o meio cibernético se tornou o principal ambiente responsável por manter as relações sociais, e onde os indivíduos passam a maior parte do tempo, compartilhando dados e informações de qualquer natureza.

Ainda segundo Lima, (2024, p. 11):

> essas mudanças não promoveram apenas benefícios às atividades diárias, mas concomitantemente, inúmeras ameaças aos bens jurídicos, visto que se trata de um espaço em que não é possível manter um controle e fiscalização em decorrência de sua alta volatilidade, abrindo deste modo, diversas oportunidades para a prática de crimes cibernéticos.

Dessarte, o ser humano moderno está inserido em um contexto onde o desenvolvimento dos meios digitais cresce de modo exponencial, ou seja, sem medida. Além disso, as atividades diárias são demasiadamente pragmáticas, basta apenas um clique ou o acionamento de um dispositivo eletrônico para que seja possível obter: comidas, roupas, pagar faturas ou conhecer uma pessoa, por exemplo, tudo se tornou muito rápido, prático, porém, frágil e também líquido, assim como dizia *Zygmunt Bauman*, "modernidade líquida" que se manifesta também no ambiente digital. Tais transformações ocasionaram modificações significativas em escala mundial, não apenas no que se refere ao avanço tecnológico e ao seu elevado consumo, mas também na maneira de pensar dos indivíduos e, consequentemente, em seus comportamentos e atitudes. As pessoas passaram a adotar ações repetitivas e mecanizadas, inseridas em um ciclo intensamente vicioso e dependente, característico da era digital.

É perceptível que diante dessa praticidade toda de forma concomitante, surgem os diversos riscos, à vista que os usuários utilizam da rede de computadores de maneira descontrolada, imprudente e demasiadamente expõem suas informações pessoais e dados muita das vezes a desconhecidos em dispositivos conectados, tal comportamento, vem desencadeando cada vez mais na presença de terceiros e agentes criminosos que se aproveitam de falhas, descuidos, de um mero vacilo, para obter benefícios ilicitamente por meio da expertise. A *Internet*, ao mesmo tempo em que representa um marco no desenvolvimento humano e na democratização do acesso à informação, também se consolidou como um terreno fértil para a prática de condutas ilícitas. O ambiente virtual, caracterizado pela rapidez na comunicação, pela amplitude no alcance das informações e pela

aparente sensação de anonimato, favorece a ocorrência de delitos que violam bens jurídicos fundamentais, tais como a intimidade, a privacidade, a honra e o patrimônio.

Segundo a Câmara dos Deputados, os primeiros crimes informáticos surgiram nos Estados Unidos na década de 1960, envolvendo práticas como sabotagem e espionagem. Estudos sistemáticos sobre o tema passaram a ocorrer apenas na década de 1970, e, a partir dos anos 1980, esses delitos se tornaram mais frequentes, abrangendo manipulação de dados bancários, pirataria de *softwares*, fraudes em telecomunicações e crimes de natureza sexual, como pornografia infantil.

No contexto do Direito Penal e Processual Penal, o avanço do meio virtual tem exigido novas regulamentações para enfrentar as consequências negativas da ampla difusão da informação, embora a *internet* facilite o acesso e a comunicação, também se tornou um espaço favorável à prática de ilícitos e à impunidade. Apesar da expressão popular de que "a *internet* é uma terra sem lei", existe amparo jurídico e penalidades para quem utiliza esse ambiente para violar direitos alheios e quando realmente forem rastreados ou encontrados, irão entender de fato que não existe anonimato para crimes no meio digital.

2.1 O SURGIMENTO DO CONCEITO CIBERNÉTICO NO BRASIL

Diferentemente dos Estados Unidos da América, onde a *Internet* surgiu com fins militares, no Brasil seu desenvolvimento teve origem na área educacional. Em 1988, instituições como a Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP), a Universidade Federal do Rio de Janeiro (UFRJ) e o Laboratório Nacional de Computação Científica (LNCC) estabeleceram as primeiras conexões com universidades norte-americanas, por meio da rede *Bitnet*, marcando o início da integração acadêmica digital no País. Com o apoio do Ministério da Ciência, Tecnologia e Inovação (MCTI), foi criada, em 1989, a Rede Nacional de Pesquisa (RNP), responsável por expandir a infraestrutura tecnológica e conectar as universidades federais, consolidando a base da *Internet* brasileira[1]. No tocante, conforme Lima (2024), na década de 1990, o acesso ainda era restrito à comunidade acadêmica e governamental, até que, em 1994, a *Internet* passou a ser disponibilizada comercialmente, tornando-se acessível ao público. Esse avanço foi intensificado com a popularização das redes sociais — como *Fotolog*, *MySpace, LinkedIn* e, principalmente, o *Orkut* — que transformaram o modo de interação e exposição de dados pessoais das pessoas.

Essa nova realidade digital deu origem à chamada "cibercultura", caracterizada pela fusão entre tecnologia e vida social, em que a comunicação, o trabalho e as relações humanas se reconfiguraram no espaço virtual. Contudo, o crescimento acelerado desse ambiente trouxe também desafios relacionados à privacidade, à segurança e à conscientização dos usuários. A consolidação do

espaço cibernético no Brasil foi impulsionada pela Portaria n.º 148/1995, que autorizou a privatização dos serviços de *Internet,* rompendo o monopólio estatal e ampliando o acesso à população. Desde então, o país passou a integrar de forma definitiva a era digital, inserindo-se em uma nova dinâmica cultural, social e tecnológica que molda até hoje o comportamento e as relações humanas. A legislação brasileira tem enfrentado desafios constantes para acompanhar o ritmo acelerado da transformação tecnológica e, por conseguinte, a complexificação dos crimes cibernéticos.

Esse cenário torna-se ainda mais desafiador quando se observa a natureza transnacional dessas infrações, que frequentemente ultrapassam fronteiras e demandam uma atuação jurídica com alcance extraterritorial. É interessante expor também que a promulgação da Lei n.º 12.965/2014, o chamado Marco Civil da *Internet* (MCI), representou um importante avanço pois foi a primeira legislação que tratou especificamente do ambiente virtual e que estabeleceu princípios, garantias, direitos e deveres para o uso da *internet* no Brasil, especialmente no tocante à proteção da privacidade e à neutralidade da rede, antes todos os temas virtuais eram tratados à luz da Constituição Federal de 1988.

Conforme essa lei primordial, fica evidente a proteção assegurada a cada usuário conectado à *internet*, como se observa no artigo 7º, inciso I a seguir:

> art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
> I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;

Contudo, Calgaroto (2021) destaca que, apesar de seus avanços, ainda persistem lacunas significativas, sobretudo no que diz respeito à responsabilização civil e à efetiva tutela dos direitos dos usuários diante de práticas ilícitas no ambiente digital. Ademais, observa-se a persistência de omissões legislativas quanto a determinados tipos penais virtuais, notadamente àqueles que atentam contra a honra e a dignidade humana.

Segundo Lima (2024, p. 23) há diversas denominações utilizadas para classificar os crimes cibernéticos, conforme se pode visualizar a seguir:

> O crime cibernético possui múltiplas denominações, entre suas variantes: crimes eletrônicos, cibercrimes, crimes virtuais, delitos informáticos, entre outros. Trata-se de condutas ilícitas onde o agente, através dos meios computacionais, digitais, dispositivos informáticos, etc., utilizando-se dos meios tecnológicos para atingir diretamente ou indiretamente os bens jurídicos.

Ainda nesse raciocínio, é relevante destacar que a legislação brasileira não utiliza expressamente o termo “crimes cibernéticos”. Essa expressão é comumente encontrada apenas em doutrinas, artigos, pesquisas e estudos especializados, enquanto o ordenamento jurídico faz referência ao crime de “invasão de dispositivo informático”, previsto no artigo 154-A do Código Penal.

Todavia, a legislação ainda se mostra bastante vaga e limitada, uma vez que não há a tipificação específica de todas as condutas relacionadas aos chamados *cybercrimes*, o que revela uma lacuna normativa ainda existente no sistema jurídico brasileiro

Apesar das deficiências existentes, há esforços legislativos recentes voltados à modernização normativa. Como se destaca a relevância da Lei n.º 14.155/2021, que alterou o Código Penal para incluir de forma mais precisa de tornar mais grave os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet, refletindo a tentativa do legislador em atualizar o sistema jurídico diante das novas modalidades de fraude eletrônica.

Nesse mesmo sentido, é possível analisar a eficácia limitada da Lei n.º 12.737/2012, conhecida como "Lei Carolina Dieckmann", foi a primeira norma brasileira voltada especificamente ao enfrentamento dos crimes cibernéticos, criada após o caso de grande repercussão envolvendo o vazamento de fotos íntimas da atriz que lhe deu nome. Contudo, sua eficácia tem se mostrado limitada, evidenciando que, mesmo após mais de uma década, é necessário revisar e atualizar periodicamente a legislação para que ela acompanhe o ritmo acelerado das inovações tecnológicas. O crescimento contínuo dos delitos digitais reforça a importância de um entendimento técnico claro sobre esses crimes, garantindo a correta aplicação das normas, a punição dos infratores e a proteção efetiva das vítimas.

3 CRIMES CIBERNÉTICOS E OS DESAFIOS DA INVESTIGAÇÃO FORENSE NO MUNDO DIGITAL NO SÉCULO XXI

Na sociedade contemporânea, observa-se que o indivíduo é constantemente incentivado pelas mídias sociais a permanecer conectado e a expor aspectos de sua vida pessoal de forma quase ininterrupta — desde o momento em que acorda até a hora de dormir. No entanto, essa prática ultrapassa o simples compartilhamento de rotinas: o ser humano tem gradativamente perdido sua essência, sua privacidade e, muitas vezes, sua saúde emocional, em busca de aceitação e validação virtual. Com o uso cada vez mais intenso das redes, o volume de informações pessoais disponibilizadas na *Internet* cresce de maneira exponencial, tornando os usuários mais vulneráveis a ataques, golpes e manipulações digitais. Dessa forma, quanto maior a exposição e a frequência de uso das redes, maior também será o número de crimes cibernéticos, uma vez que o ambiente digital se torna terreno fértil para práticas ilícitas que se aproveitam da distração, confiança e inocência dos usuários.

Mas afinal, o que são os crimes cibernéticos? de acordo com Queiroz (2024, p. 419), os "crimes cibernéticos são aqueles que no contexto da atividade criminal são cometidos ou facilitados

pela rede mundial de computadores (*Internet*), assim como pelo abuso ou mau uso de sistemas e aplicativos diversos". Sabe-se que o grande perigo dos crimes no ambiente digital é a sua transnacionalidade, não importa a cidade, estado ou país, o agente criminoso poderá praticar o delito contra qualquer pessoa conectada ou não à rede mundial de computadores, assim, quanto maior a habilidade técnica de quem pratica a conduta, mais fácil e rápido será burlar os meios digitais e legais. No tocante, conforme Queiroz (2024, p. 420):

> os crimes cibernéticos dividem-se em "crimes cibernéticos impróprios" e "crimes cibernéticos próprios". Os primeiros, podem ser praticados da forma tradicional ou por intermédio de computadores, ou seja, o computador apresenta-se apenas como meio para a prática do crime, como no caso dos delitos de ameaça, racismo, estelionato, crimes contra a honra, falsificação de documentos, dentre outros previstos no Código Penal e em legislações esparsas. Os "crimes cibernéticos próprios" somente podem ser praticados com a utilização de computadores ou qualquer outro dispositivo eletrônico que possibilite o acesso à *Internet*. O meio informático é o instrumento utilizado para a pratica do crime e também, a depender do tipo penal cometido, e do bem jurídico tutelado. É a hipótese do art.154 - A (invadir dispositivo informático alheio), art.313-A (inserção de dados falsos em sistema de informações) além de outros existentes na legislação penal vigente.

É possível elencar os crimes cibernéticos mais comuns, que abrangem condutas cada vez mais sofisticadas, dentre eles são: estelionato virtual, crimes contra a honra, *cyberbullying, oversharing, stalking*, *sextorsão, phishing,* fraude bancária eletrônica, *fake news,* espionagem digital, tráfico de drogas e armas pela *dark web*, pornografia infantil, induzimento ao suicídio no meio digital entre outros. Conforme palavras de De Oliveira (2022, p. 12) "sem dúvidas, os crimes contra o patrimônio são os mais comuns no ambiente virtual. Dentre esses, o de maior destaque é o estelionato". A exemplo disso, indivíduos maliciosos estão produzindo sites de vendas com informações falsas de modo que induzem as pessoas a pagar por produtos que não existem. Acerca do estelionato o Artigo 171 do Código Penal aborda o seguinte:

> art. 171 – "obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento: Pena – reclusão, de um a cinco anos, e multa". (Brasil, 1940)

Sobre esse aspecto menciona Lima (2024, p. 21), alguns termos em *inglês* que descrevem práticas criminosas atuais no ambiente digital:

> em vista disso, termos como: "*stalking*", "*sexting",* "*cyberbullying*", "*oversharing*", são apenas alguns exemplos de práticas realizadas pelos próprios internautas as quais envolvem perseguição e exposição excessiva não apenas de seus dados pessoais, mas inclusive conteúdos íntimos. Deste modo, os cibercriminosos obtém facilmente o conhecimento das vulnerabilidades oferecidas pelos próprios usuários, pois no espaço cibernético é muito comum a presença de perfis falsos para realização desse tipo de conduta.

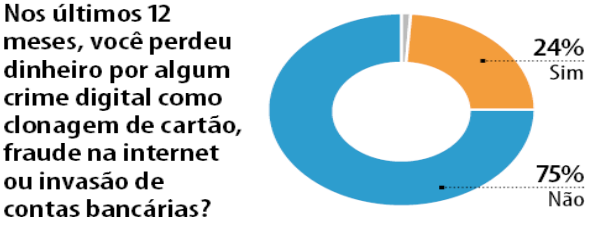
Há também a prática do *phishing*, que consiste no envio massivo de *e-mails* ou mensagens que induzem a vítima a clicar em *links* maliciosos, permitindo a instalação de *malwares* capazes de

capturar dados sensíveis, como senhas bancárias. Por outro lado, tem o *hacking,* que envolve o acesso não autorizado a sistemas com o objetivo de roubar, alterar ou destruir informações, podendo ser motivado por ganho financeiro, espionagem ou desafio intelectual. Para isso, *hackers* exploram vulnerabilidades de *softwares* ou utilizam técnicas de engenharia social para obter credenciais de acesso.

Dessarte, é notório que o ordenamento jurídico brasileiro não possui uma norma penal unificada que concentre os tipos penais cibernéticos ao quais se encontram localizados em leis esparsas, como na Lei Carolina Dieckmann (Lei 12.737/2012), Código Penal (art. 122, § 4º, art. 141, § 2º, art.154-A e art. 218-C), Lei n.º 14.155/2021 (aumento da pena), Projeto de Lei n.º 4.658/24, incluindo também a Convenção de *Budapeste* de 2023 e o Tratado das Nações Unidas de 2025, entre outras normas legais relevantes.

É importante destacar que inúmeros crimes cibernéticos praticados habitualmente sequer são investigados. Isto acorre não apenas pela falta de capacitação das autoridades que recebem a notícia do crime, como por vezes, pela ausência de ferramentas forenses adequadas para a extração e análise dos dados pertinentes. Contudo, o principal entrave reside na insuficiência de profissionais especializados e na escassa atenção destinada a essa problemática. Diante disso, a investigação forense no meio digital enfrenta muitos desafios, entre eles é o de iniciar o procedimento de forma qualitativa, ainda que, na maioria das vezes, sem nenhum êxito na identificação da autoria dos perfis criminosos.

Diante disso, é tão relevante e preocupante essa situação, pois o Brasil ocupa o segundo lugar no *ranking* mundial de ataques cibernéticos, registrando 1.379 golpes por minuto — mais de 700 milhões de pessoas em apenas 12 meses, conforme o Panorama de Ameaças para a América Latina 2024. O dado revela a gravidade da situação e reforça que, além do uso de tecnologias de proteção, é essencial que os usuários invistam em capacitação e conscientização digital, para reduzir riscos e fortalecer a segurança no ambiente virtual. Nesse mesmo embalo, segundo pesquisa realizada pelo DataSenado, revelou que 24% dos brasileiros com mais de 16 anos já foram vítimas de algum golpe digital. O levantamento também estima que mais de 40 milhões de pessoas no país perderam dinheiro em decorrência de crimes cibernéticos, evidenciando a dimensão e o impacto econômico desses delitos na sociedade brasileira, como pode visualizar abaixo:



Fonte: Instituto de Pesquisa DataSenado

Sob essa ótica, os dados estatísticos evidenciam que a sofisticação crescente das práticas criminosas no meio digital reforça a necessidade de maiores investimentos em cibersegurança, ações de educação preventiva, fortalecimento legislativo e maior atuação da perícia forense em todos os estados brasileiros. Em consonância, mesmo que 75% não tenham sofrido perdas financeiras eletronicamente, essa tendência de expansão da criminalidade digital demonstra uma extrema urgência de medidas e posturas jurídicas mais eficazes para reduzir essa problemática instalada na sociedade.

Segundo dados internacionais, o Brasil ocupava, em 2019, o terceiro lugar no *ranking* dos países mais atingidos por ataques cibernéticos, atrás apenas da China e dos Estados Unidos, conforme relatório da *Symantec Endpoint Protection (SEP)*. À vista disso, com a pandemia de *Covid*-19, em 2020, esses números aumentaram significativamente. De acordo com o *Fortinet Threat Intelligence Insider Latin America*, o país registrou mais de 3,4 bilhões de tentativas de ataques somente entre janeiro e setembro de 2020, demonstrando o rápido crescimento e a gravidade da exposição brasileira às ameaças digitais. Em sintonia, o Corregedor Nacional de Justiça, ministro Humberto Martins, afirmou que o isolamento social imposto pela pandemia de *Covid*-19 reduziu significativamente os índices de roubos e furtos nas cidades brasileiras, em razão da menor circulação de pessoas. Contudo, esse mesmo cenário favoreceu o crescimento de outras modalidades criminosas, especialmente os crimes cibernéticos, que se intensificaram durante esse período.

No tocante, é preocupante o aumento que os crimes cibernéticos têm tido no País, e por esse motivo, deve se ter uma atenção redobrada para o combate dessa problemática tão alarmante. À vista disso, se tem observado a ocorrência demasiada de golpes cibernéticos envolvendo tanto pessoas físicas quanto jurídicas no ano de 2025. Em diversos casos, tem acontecido o "golpe do falso advogado", em que criminosos se passam por advogados de forma ardilosa ou até mesmo advogados com má-fé, mediante acesso indevido a processos de advogados/ou de outros advogados, entram em contato com clientes, solicitando pagamentos, transferências ou envio de documentos, muita das vezes dando a falsa notícia de que tal processo teve êxito, ou que foi deferido pelo juiz, e o cliente acredita ser de fato o seu advogado e acaba realizando o pagamento e sendo prejudicado. Esses golpes são sofisticados, planejados, infelizmente, na maioria das vezes de difícil detecção e solução, deixando a vítima totalmente desamparada e com profundos abalos emocionais.

O Conselho Nacional de Justiça (CNJ) tornou obrigatória a autenticação em dois fatores (MFA) no Processo Judicial Eletrônico (PJe), conforme a Portaria n.º 140/2024, visando aumentar a segurança dos sistemas judiciais e reduzir fraudes como o "golpe do falso advogado". A medida aplica-se a usuários externos — advogados, partes e demais interessados — que acessam o PJe, o Jus.Br e a Plataforma Digital do Poder Judiciário Brasileiro (PDPJ), exigindo, além do login e senha,

um código gerado por aplicativo autenticador. A iniciativa integra um plano mais amplo do CNJ para aprimorar a proteção de dados e fortalecer o acesso seguro às plataformas digitais. Para evitar fraudes, o CNJ e a Ordem dos Advogados do Brasil (OAB) orientam os usuários a verificar a identidade profissional no site da OAB ou no ConfirmADV, desconfiar de mensagens urgentes ou *links* suspeitos e consultar sempre o processo diretamente no site oficial do tribunal.

Sabe-se que as fraudes digitais têm se intensificado com o envio de links e arquivos malicioso por aplicativos de mensagens, que induzem a vítima a permitir acesso remoto aos seus dados pessoais e bancários. Com essas informações, criminosos conseguem invadir contas e realizar transferências de forma rápida e quase sempre irreversível. Trata-se de uma típica prática de "engenharia social", na qual "iscas" são usadas para obter informações sigilosos. Por isso, é essencial que os usuários adotem medidas de proteção, como evitar clicar em *link* suspeitos, não abrir anexos desconhecidos e confirmar a autenticidade de qualquer solicitação antes de fornecer dados pessoais.

A Polícia Civil de São Paulo, por meio da 2ª Delegacia da Divisão de Crimes Cibernéticos (DCCIBER), esclareceu o maior ataque *hacker* já registrado no país, que resultou no desvio de R$ 541 milhões por meio de operações fraudulentas via Pix. As investigações apontaram que um operador de TI da empresa C&M *Software* — responsável por intermediar transações entre o Banco do Futuro (BMP) e o Banco Central — foi cooptado por criminosos e permitiu o acesso indevido ao sistema, viabilizando transferências eletrônicas em massa para diversas instituições financeiras. O funcionário confessou sua participação e foi preso, enquanto a polícia continua a identificar e localizar os demais envolvidos na ação criminosa.

Também é importante mencionar o crescente número de ocorrências do chamado "golpe da voz roubada" ou "golpe da ligação muda", que se tornou um dos crimes digitais mais frequentes na atualidade. Nesse tipo de fraude, os criminosos entram em contato com a vítima, gravam ou clonam sua voz e, com o uso de tecnologias de Inteligência Artificial (IA), reproduzem falas falsas e convincentes. Em seguida, entram em contato com familiares, amigo ou conhecidos da vítima, simulando situações de urgência para solicitar transferências de dinheiro ou dados pessoais. Atinente, esse golpe tem se disseminado rapidamente devido à facilidade de manipulação de áudios com IA, com o uso do *deepfake* de voz, o que torna as falsificações extremamente realistas e, consequentemente, dificulta a identificação da fraude pelas vítimas desses crimes.

Diante disso, muitos golpistas se passam por autoridades públicas ou representantes de instituições privadas, o que faz com que a probabilidade de as pessoas caírem em fraudes seja extremamente alta. Diante dessa realidade, a polícia e especialistas em segurança digital recomendam uma série de medidas preventivas, tais como: não atender ligações provenientes de números desconhecidos ou suspeitos, confirmar diretamente com o órgão ou empresa mencionada a

veracidade do contato, optar por chamadas de vídeo para verificar a identidade do criminoso, desconfiar de solicitações com tom de urgência e comunicar imediatamente o fato às autoridades competente. Além disso, orienta-se as famílias estabelecerem uma palavra-chave de segurança entre si, a fim de evitar ser vítimas de golpes desse tipo.

Segundo Queiroz (2024), a investigação de crimes cibernéticos exige cuidados preliminares específicos, sobretudo o imediato pedido de preservação dos dados digitais junto aos provedores, já que esse tipo de prova é altamente volátil e, uma vez removida, dificilmente pode ser recuperada. Por essa razão, a apuração de delitos virtuais diferencia-se significativamente das demais investigações criminais, sobretudo no que se refere à coleta, conservação e manutenção da cadeia de custódia, elementos essenciais para garantir a autenticidade e a validade jurídica das evidências digitais

Nota-se que os delitos cibernéticos atingem não apenas cidadãos comuns, mas também o próprio Estado, colocando em risco informações sensíveis e a segurança nacional. Entretanto, a lentidão do sistema judiciário em investigar, processar e punir esses crimes ainda representa um grande obstáculo, contribuindo para a sensação de impunidade e para a continuidade dessas práticas no ambiente digital.

4 O PERFIL DO CRIMINOSO E AS CARACTERÍSTICAS DOS CIBERCRIMES

Domingos e Jacob (2024, p. 3), acreditam que “para entender o perfil dos criminosos cibernéticos e outras características destes, é essencial compreender a linha do tempo histórica da *internet*. Ambiente onde essas atividades ilegais se consumam, principalmente por conta da alta possibilidade de camuflagem dos indivíduos”.

É importante destacar conforme Lima (2024, p. 19):

> que o agente criminoso pode se inserir de diversas maneiras quando se trata do meio digital, diferentemente das práticas ocorridas no mundo físico. Invadir sistemas através de vírus, captar e roubar dados pessoais, apresentar falsidade ideológica e ter acesso a informações confidenciais, são apenas alguns dos inúmeros delitos desenvolvidos no espaço cibernético. Além disso, está cada vez mais difícil traçar o perfil de um criminoso na *Internet*, pois não se sabe precisamente como o delito foi arquitetado em virtude das diversas possibilidades que o agente possui de se ocultar através do anonimato, e por consequência, lograr impunidade.

Destarte, a facilidade para o cometimento de delitos é tão expansiva que mesmo se o indivíduo não for um agente criminoso na vida real e perceber a inclinação de se camuflar no mundo virtual, acaba por se sentir mais seguro para praticar o fato transgressor. Cadilhac (2022) acredita, que ao se analisar este contexto pode observar que existe um conjunto de características que contribuem para o rápido crescimento e disseminação de crimes digitais, visto que sua fonte basilar se deriva da facilidade de escalabilidade, acessibilidade aos meios para prática do crime, o

anonimato, portabilidade e capacidade de transferência, alcance em escala global, e ausência de vigilância capacitada.

Em sintonia com Lima (2024, p. 25), “o anonimato é uma das principais barreiras encontradas pelos legisladores para detectar o sujeito ativo, conforme supracitado, desta forma, o mesmo torna-se apto a destilar ódio, ofensas e ferir, inclusive, a dignidade da pessoa humana através de perfis falsos na esfera cibernética”. Nesse sentido, em harmonia, Cadilhac (2022), salienta que muitos criminosos digitais acreditam que permanecerão anônimos, sobretudo porque o poder público ainda carece de preparo técnico e estrutural suficiente para produzir provas sólidas e fundamentar adequadamente uma condenação.

Nesse cenário, a prova pericial assume papel central, pois é justamente a combinação entre a atuação de profissionais altamente qualificados e o uso de tecnologias avançadas que se revela determinante para o êxito das investigações. Esse conjunto garante que os vestígios digitais sejam adequadamente coletados, analisados e validados, permitindo sua admissibilidade em juízo.

É notório que no mundo digital, os criminosos utilizam uma variedade de técnicas sofisticadas para explorar vulnerabilidades em sistemas e usuários. Por meio de ataques cibernéticos, como *phishing, ransomwaree, malwares*, conseguem efetuar roubos de dados pessoais, bancários e informações sensíveis das pessoas.

Como disse Pinheiro (2023, p. 392):

> o maior problema jurídico dos crimes virtuais ainda é o fato de que os criminosos estão sempre um passo à frente. Há necessidade de investir mais no preparo da polícia para que tenham mais ferramentas para realizar perícia forense, bem como também em campanhas educativas da população, para que o cidadão saiba se defender melhor dos novos tipos de golpes e ameaças digitais. Além disso, a ação rápida, para pegar o "bandido com a mão na máquina", é essencial. Ainda há bastante dificuldade de gerar prova de autoria quando o crime ocorre pela *Internet*. Outro desafio é o de rever a legislação penal, para que alguns tipos penais passem por atualização e aumento de pena.

5 FORMAS INVESTIGATIVAS DE COMBATE À CRIMINALIDADE DIGITAL

Segundo Queiroz (2024), a criminalidade digital configura-se como um fenômeno complexo e em constante evolução, demandando métodos investigativos adaptados às particularidades do ambiente virtual. Diferentemente dos delitos tradicionais, os cibercrimes frequentemente utilizam tecnologias avançadas para ocultar rastros e dificultar tanto a identificação de seus autores quanto a coleta de provas. Por essa razão, o combate a essas infrações exige estratégias sofisticadas, capazes de integrar técnicas investigativas clássicas a recursos tecnológicos inovadores.

Cadilhac (2022), afirma que, com o avanço digital ficou mais fácil cometer crimes por meios virtuais, o que exigiu a criação de uma polícia especializada — a *cyber* inteligência. Apesar da falsa

sensação de anonimato proporcionada pela “tela”, delitos cibernéticos deixam rastros (endereços IP, *cookies, logins,* arquivos etc.) que podem ser registrados e periciados. Peritos forenses digitais, com profundo conhecimento de sistemas operacionais e *softwares*, são capazes de decifrar esses vestígios e identificar crimes e autores, reforçando a eficácia das investigações.

No Brasil são utilizados alguns programas para investigação como o IPED – Indexador e Processador de Evidências Digitais, que é um *software* desenvolvido pelo Perito Criminal Federal e professor Luís Filipe, com o apoio de outros peritos, para a investigação da Operação Lava Jato. Ele permite recuperar arquivos deletados, localizar palavras, detectar nudez, rastrear localidades, identificar criptografia, cruzar informações, etc. Com *softwares* de análise, coleta e investigação de provas, quando utilizadas da forma correta, pelos peritos competentes, vão garantir que a cadeia de evidências não seja quebrada e obtenha-se o juízo de admissibilidade, aumentando a probabilidade de uma convicção ao final do processo.

Além da investigação direta, a análise estratégica da informação torna-se essencial: mapear redes criminosas, identificar vulnerabilidades em sistemas e propor medidas preventivas são passos fundamentais. Assim, o sucesso das investigações cibernéticas depende não apenas da técnica, mas de uma visão ampla que una tecnologia, legislação e inteligência estratégica, tornando o combate à criminalidade digital mais preciso e eficaz. Em uma analogia ao personagem *Sherlock Holmes*, que usa a observação minuciosa, a dedução lógica e o conhecimento detalhado para solucionar casos aparentemente insolúveis — muitas vezes notando aquilo que a própria polícia ignora —, o perito digital precisa atuar de forma semelhante no ambiente cibernético. Ele analisa cada vestígio digital, por menor que pareça, buscando reconstruir a trajetória do crime e trazer à tona o perfil do criminoso.

5.1 CYBER INTELIGÊNCIA E INTELIGÊNCIA ARTIFICIAL (IA): ESTRATÉGIAS E DESAFIOS NO COMBATE ÀS AMEAÇAS CIBERNÉTICAS

A *Cyber* Inteligência consiste na coleta, análise e interpretação de dados digitais com o objetivo de prevenir e combater ameaças no ambiente virtual. Sua aplicação permite monitorar atividades suspeitas, antecipar ataques e fornecer subsídios estratégicos para autoridades competentes. Quando integrada à Inteligência Artificial (IA), os sistemas de *Cyber* Inteligência são capazes de processar grandes volumes de dados em tempo real, detectando anomalias que poderiam passar despercebidas pela observação humana. Essa sinergia entre tecnologia e investigação amplia significativamente a capacidade de resposta a cibercrimes, reduzindo riscos e o tempo de reação.

Contudo, o uso da IA no enfrentamento da criminalidade digital apresenta desafios relevantes, a interpretação automatizada de dados pode gerar falsos positivos, comprometendo investigações e a

responsabilização adequada de indivíduos inocentes. Além disso, a implementação de sistemas inteligentes requer investimentos contínuos, treinamento especializado e atualização constante frente a técnicas cada vez mais sofisticadas de ataque, como *deepfakes* e *ransomwares* avançados. O equilíbrio entre eficiência tecnológica e proteção de direitos fundamentais constitui, portanto, um desafio central para o Estado. Outro aspecto crítico envolve a ética e a legalidade no emprego de *cyber* inteligência e IA. A coleta de informações deve respeitar a privacidade dos cidadãos e os princípios constitucionais, prevenindo abusos e violações de direitos humanos. Para tanto, é essencial a definição de normas claras sobre o alcance das atividades de monitoramento, assegurando que os sistemas de IA sejam transparentes, auditáveis e responsáveis.

Conforme Padilha et al. (2021), para que análises aprofundadas possam ser realizadas, no entanto, é necessário assegurar que as informações necessárias para entender o que aconteceu sejam recuperadas e organizadas, de modo que o perito chegue a conclusões verdadeiras. Dessa forma, a conjugação entre *Cyber* Inteligência e IA constitui um pilar estratégico na segurança digital, exigindo integração multidisciplinar, governança eficaz e constante atualização tecnológica.

5.2 LEGISLAÇÃO PUNITIVA E DESAFIOS NA QUALIFICAÇÃO DE CIBERCRIMES NO PAÍS: NECESSIDADE DE APERFEIÇOAMENTO LEGAL E RIGOR NA APLICAÇÃO

A legislação brasileira ainda enfrenta dificuldades para acompanhar a complexidade e a rapidez da evolução tecnológica. Apesar de avanços como a Lei n.º 12.737/2012 (Lei Carolina Dieckmann), Lei n.º 14.155/2021(agravantes de crimes informáticos), e a Lei n.°13.709/2018 (Lei de Proteção de Dados), que tratam de crimes cibernéticos e da proteção do direito de intimidade e de privacidade de informações pessoais. Muitos tipos de delitos ainda carecem de definição precisa e de critérios claros de tipificação. A ausência de normas detalhadas dificulta a atuação do judiciário e gera insegurança jurídica, prejudicando a punição adequada dos criminosos digitais.

Nesse sentido, o aperfeiçoamento legal passa, portanto, pela atualização contínua das leis existentes, pela criação de tipificações claras e pelo estabelecimento de procedimentos processuais adaptados à realidade digital que se tem enfrentado. É essencial que o legislador preveja medidas preventivas, mecanismos de cooperação internacional e instrumentos tecnológicos de coleta e preservação de provas digitais, garantindo uma resposta eficaz aos crimes cibernéticos.

Além disso, o rigor na aplicação da lei deve ser equilibrado com a proteção dos direitos humanos, evitando abusos de poder ou violação da privacidade. A legislação deve, assim, ser compreensiva, flexível e capaz de acompanhar a evolução tecnológica sem perder de vista os princípios constitucionais, garantindo justiça, segurança e proporcionalidade na repressão aos

cibercrimes. Dessa forma, vale destacar que, no Brasil, existem disposições legais que garantem a proteção das pessoas vítimas de atos ilícitos relacionados a cybercrimes, assegurando seus direitos e meios de reparação frente aos danos sofridos.

Nessa linha, observa-se que a legislação brasileira tem se adaptado às demandas do meio digital por meio de alterações relevantes no Código Penal, sobretudo para enfrentar a gravidade e complexidade dos crimes cibernéticos. O art. 141, §2º, prevê a aplicação tripla da pena nos crimes contra a honra praticados ou divulgados em redes sociais, dada a amplitude e o impacto da disseminação *on-line.* O art. 122, §4º, traz a possibilidade do aumento da pena até o dobro para os casos de induzimento ou instigação ao suicídio cometidos por meios digitais, reconhecendo o elevado potencial lesivo dessas condutas. Já o art. 171, §§2º-A e 2º-B, introduz qualificadoras específicas para fraudes eletrônicas praticadas mediante engano em redes sociais, contatos telefônicos, e-mails falsos ou com uso de servidores estrangeiros, amplificando o rigor punitivo e reafirmando que os cybercrimes são crimes complexos e de rápida proliferação demandando respostas mais robustas do que os delitos tradicionais.

É indispensável destacar o Projeto de Lei n.º 4.658/24, proposto pelo Deputado Federal Paulo Litro, que atualmente se encontra em tramitação na Câmara dos Deputados, apresenta-se como uma resposta significativa ao avanço da criminalidade digital no Brasil. Embora o projeto ainda aguarde aprovação do Congresso Nacional, ele já resultou em alterações no Código Penal, incluindo os acréscimos ao Art. 62, V (“praticar o delito através da internet ou por meios digitais”) e ao Art. 141, V (“por meio da *Internet* ou através de meios digitais”). A proposta busca majorar as penas para todos os crimes cometidos no ambiente virtual, ampliando o rigor punitivo e adequando o ordenamento jurídico às novas formas de ilícitos digitais. Apesar de existirem normas importantes em vigor, persistem lacunas relevantes na tipificação de condutas praticadas *on-line*, evidenciando que o atual Código Penal ainda não acompanha plenamente a complexidade dos delitos cibernéticos. Nesse contexto, o projeto surge como uma alternativa promissora ao fortalecer a proteção às vítimas, reforçar a prevenção e alinhar o país aos padrões internacionais de enfrentamento aos cibercrimes. Além disso, ao se observar a penalidade já vigente para crimes contra a honra cometidos no meio digital — cuja pena é triplicada —, percebe-se a possibilidade de estender esse tratamento mais rigoroso a todos os delitos digitais, contribuindo para a modernização do sistema penal e para uma resposta mais eficaz diante das crescentes ameaças cibernéticas.

6 A IMPORTÂNCIA DOS PERITOS FORENSES NA DETECÇÃO E EMBATE DE DELITOS CIBERNÉTICOS

Os peritos forenses desempenham papel fundamental na investigação de crimes cibernéticos, atuando na coleta, análise e preservação de provas digitais. Sua função vai muito além da simples extração de dados; envolve interpretação técnica, validação das evidências e apresentação dos resultados em conformidade com padrões legais, garantindo que as provas sejam admissíveis em juízo.

O trabalho desses profissionais se mostra essencial em casos de elevada complexidade, como invasões de sistemas, fraudes bancárias e crimes envolvendo *blockchain.* A perícia permite rastrear transações digitais, identificar os responsáveis e reconstruir a sequência de eventos, transformando dados aparentemente abstratos em evidências concretas. Para tanto, é necessário domínio das tecnologias emergentes, conhecimento de protocolos de segurança e aplicação de metodologias reconhecidas internacionalmente, garantindo a confiabilidade dos resultados. Contudo, a crescente complexidade tecnológica impõe desafios significativos. A constante atualização dos peritos, somada a investimentos em laboratórios especializados e tecnologias avançadas, é essencial para que a perícia acompanhe a evolução dos crimes digitais. A falta de recursos humanos e técnicos compromete a agilidade e a precisão das investigações, reforçando a necessidade de políticas públicas que fortaleçam a perícia forense digital no Brasil.

Nesse sentido, trazendo para o âmbito mais próximo, em Ariquemes/RO, o crime cibernético mais recorrente é o estelionato, conforme informações da Delegacia de Polícia Civil e da Politec. As autoridades locais enfrentam graves limitações estruturais, como a falta de equipamentos tecnológicos e de profissionais especializados em investigação forense digital. Por essa razão, a maioria dos casos é encaminhada para Porto Velho/RO, o que retarda as investigações e reduz sua eficácia. O perito criminal Artur Santana destaca ainda que há uma perita responsável pela área de Tecnologia da Informação (TI), além de uma grande carência de recursos e profissionais suficientes e capacitados no combate aos crimes cibernéticos no Estado de Rondônia. Essa realidade evidencia a fragilidade do sistema de segurança no município, agravada pelo alto custo de equipamentos modernos e pela dificuldade de ingresso de novos peritos, devido à baixa frequência de concursos públicos e ao número reduzido de profissionais efetivamente contratados pelo Estado.

E para os casos de estelionatos ou outros crimes de natureza cibernética, é essencial que a vítima registre o ocorrido para possibilitar a investigação. Em Rondônia, o procedimento pode ser feito pelo Portal da Polícia Civil, onde é possível comunicar crimes virtuais em Ouvidoria/Fala.Br. Esses registros são fundamentais para que as autoridades tenham elementos para apurar os fatos e adotar as medidas cabíveis para a minimização dessa problemática constante.

O Brasil enfrenta escassez de peritos forenses especializados em crimes digitais, o que atrasa investigações, acumula processos e compromete a qualidade das perícias, prejudicando a eficiência

da Justiça. Além da falta de profissionais, a limitação de recursos financeiros dificulta a modernização dos laboratórios e a aquisição de tecnologias avançadas, essenciais para acompanhar a evolução dos delitos virtuais. A falta de infraestrutura e integração entre órgãos também torna o processo investigativo mais lento e menos eficaz.

Mas como a sociedade pode prevenir e combater o cibercrime? a prevenção e o combate ao cibercrime exigem atenção constante e adoção de práticas seguras no uso da tecnologia. Pequenas ações diárias podem fazer grande diferença na proteção de dados e na redução de riscos. Manter o *software* e o sistema operacional sempre atualizados é uma das medidas mais importantes, pois as atualizações corrigem falhas e fortalecem a segurança do dispositivo. O uso de um antivírus confiável e atualizado também é fundamental para detectar e eliminar ameaças antes que causem danos.

Outro ponto essencial é a criação de senhas fortes, complexas e exclusivas para cada conta, com trocas periódicas para evitar invasões. Além disso, deve-se evitar abrir anexos de *e-mails* suspeitos ou de origem desconhecida, pois podem conter vírus ou programas maliciosos. Da mesma forma, não clicar em *links* recebidos por *e-mails* de *spam* ou em *sites* não confiáveis ajuda a impedir o acesso a páginas fraudulentas e o roubo de informações pessoais.

Diante do crescimento exacerbado dos crimes cibernéticos, torna-se necessário que o Estado avalie a ampliação do número de vagas em concursos públicos para perito criminal especializado em Tecnologia da Informação (TI). Embora os certames contemplam diversas áreas – como odontologia, medicina, criminalística geral, TI, química e medicina veterinária – é inegável que a demanda por profissionais capacitados em informática forense tende a aumentar de forma exponencial, já que com a presença de mais peritos na área de TI, maior seria a capacidade investigativa no meio digital de crimes. E nesse mesmo raciocínio que aja mais vagas para essa carreira, que infelizmente ainda se encontra muito escassa.

6.1 PROVAS DIGITAIS E O USO DAS TECNOLOGIAS: DA PERÍCIA CIBERNÉTICA AO *BLOCKCHAIN* NO COMBATE AOS CIBERCRIMES

A visão de Queiroz (2024), é que a produção e análise de provas digitais são elementos centrais na persecução penal de crimes virtuais. Arquivos, registros de rede, *logs* de servidores e dados criptografados constituem fontes valiosas de informação, cujo manuseio requer conhecimento técnico especializado. A perícia cibernética garante que a evidência seja preservada, autenticada e apresentada de maneira que seja juridicamente válida.

O uso de tecnologias como *blockchain* (cadeia de blocos*)* tem se mostrado inovador no combate aos cibercrimes. A rastreabilidade de transações, combinada à imutabilidade dos registros,

facilita a identificação de atividades fraudulentas, lavagem de dinheiro digital e ataques a criptomoedas, atinente a isso, os peritos treinados podem explorar essas tecnologias para reconstruir fluxos financeiros e estabelecer conexões entre diferentes atores criminosos. Paralelamente, técnicas de análise forense avançada, como recuperação de dados apagados, análise de *malware* e engenharia reversa, ampliam a capacidade investigativa.

A integração dessas ferramentas permite não apenas coletar provas, mas também entender o *modus operandi* dos criminosos, fornecendo informações estratégicas para prevenir novos ataques. Entretanto, desafios legais e técnicos persistem, e a rápida evolução tecnológica exige atualização constante de protocolos de perícia e normas jurídicas. Além disso, a aplicação de ferramentas emergentes precisa equilibrar eficiência investigativa com respeito à privacidade e à legalidade, evitando abusos que possam comprometer a legitimidade das provas. Assim, destaca-se a importância da inovação constante para enfrentar métodos cada vez mais sofisticados de ataques cibernéticos.

7 A PROTEÇÃO CONSTITUCIONAL DOS DIREITOS HUMANOS FRENTE ÀS AMEAÇAS DIGITAIS

A Constituição Federal de 1988 estabelece fundamentos essenciais para a proteção da dignidade da pessoa humana, que se tornam ainda mais relevantes diante das ameaças digitais. O artigo 1º, inciso III, consagra a dignidade da pessoa humana como princípio basilar do Estado Democrático de Direito, assegurando que todos os indivíduos sejam tratados com respeito e proteção, inclusive no ambiente virtual. Crimes cibernéticos, como fraudes, golpes e estelionatos, violam diretamente essa dignidade, causando prejuízos não apenas financeiros, mas também emocionais e sociais, comprometendo a integridade psicológica das vítimas.

O princípio da prevalência dos direitos humanos, previsto no artigo 4º, inciso II, reforça a responsabilidade do Estado de proteger os cidadãos contra violências e violações de seus direitos fundamentais, inclusive no contexto digital. Nesse sentido, a legislação brasileira e os mecanismos de repressão aos cibercrimes devem ser interpretados de forma a garantir a máxima proteção às vítimas, promovendo medidas preventivas e repressivas que assegurem sua segurança, bem-estar e reparação dos danos sofridos.

Faz-se necessário mencionar o texto da Carta Magna em seu artigo 5º, caput e inciso X, da Constituição Federal de 1988, que traz o seguinte:

> 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: X- São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado

> o direito a indenização pelo dano material ou moral decorrente de sua violação (Brasil, 1988).

É importante mencionar também sobre a liberdade de expressão, assegurada pela Constituição Federal no art. 5º, IV e IX, constitui um dos pilares do Estado Democrático de Direito, garantindo a todos o direito de manifestar opiniões, ideias e pensamentos. Entretanto, esse direito não é absoluto, pois sua proteção encontra limites justamente no momento em que a manifestação ultrapassa o campo do debate legítimo e passa a violar direitos de terceiros, como a honra, a imagem, a dignidade e a privacidade. Quando a "expressão" atinge, denigre ou fere outra pessoa, deixando de exercer um direito constitucional para se transformar em ofensa, discriminação ou divulgação ilícita de conteúdo, não se trata mais de liberdade – mas do possível início de um crime. No ambiente digital essa prática se intensifica, pois a velocidade de propagação das informações amplia o alcance e o dano das condutas, tornando ainda mais evidente que a liberdade de expressão deve ser exercida com responsabilidade, sendo vedado o uso das redes com escudo para prática de crimes ou violações de direitos humanos, deixando claro que a *Internet* não é e jamais será uma terra sem lei.

Dessa forma, a proteção constitucional dos direitos humanos frente às ameaças digitais exige a integração entre normas jurídicas, atuação policial especializada, perícia forense, políticas de educação digital e apoio psicossocial. Ao assegurar a dignidade e a segurança das vítimas, o ordenamento jurídico não apenas responde aos crimes cibernéticos, mas também contribui para a construção de um ambiente virtual mais seguro e ético, reafirmando o compromisso do Estado brasileiro com os direitos fundamentais e a proteção integral da pessoa humana.

7.1 A CONVENÇÃO DE *BUDAPESTE* E O TRATADO GLOBAL DA ONU: A APLICAÇÃO DE LEIS ESTRANGEIRAS NO BRASIL CONTRA CRIMES CIBERNÉTICOS

Criada em 2001 pelos Estados membros do Conselho da Europa e os seguintes Estados signatários, a Convenção de *Budapeste* também conhecida como convenção contra a criminalidade cibernética, dispõe em seu preâmbulo o seguinte: "Convencidos da necessidade de buscar prioritariamente uma política criminal comum destinada à proteção da sociedade contra o crime cibernético, nomeadamente pela adoção de legislação apropriada e pela promoção da cooperação internacional, entre outras medidas". O Brasil promulgou a convenção em 2023, desde então, se unindo a outros países, com intuito de expandir as relações internacionais, a convenção supre lacunas na seara criminal, fornecendo parâmetros os quais contribuem com o desenvolvimento da persecução penal aos crimes que transcendem fronteiras geográficas.

Na visão de Lima (2024), é importante destacar que após a eclosão do período pandêmico, o Brasil começou a ampliar os serviços digitais e promover a inclusão desses meios aos seus cidadãos,

assim, os crimes cibernéticos se tornaram cada vez mais desenfreados, em decorrência do aumento do uso tecnológico e da necessidade de se adequar a essas circunstâncias. Em síntese, a padronização internacional dessas normas é essencial para que os países atuem de forma conjunta e alinhada aos preceitos legais, garantindo uma justiça mais célere, eficaz e adequada às necessidades atuais.

Assim, embora o Brasil ainda esteja em fase inicial de desenvolvimento quanto a sua legislação digital, a participação em uma convenção internacional de grande relevância, como a Convenção de *Budapeste*, oferece diretrizes essenciais para o enfrentamento dos crimes cibernéticos enfrentados no País. Esse instrumento internacional fornece um referencial normativo estruturado, permitindo ao país não apenas alinhar-se a padrões globais de investigação e cooperação, mas também estabelecer bases sólidas para a penalização efetiva das condutas ilícitas no ambiente digital. A adesão à Convenção fortalece, portanto, a capacidade do Estado brasileiro de combater delitos cibernéticos de forma coordenada, ética e juridicamente segura. Entendendo que há uma extrema necessidade de buscar prioritariamente uma política criminal destinada à proteção dos direitos humanos na sociedade contra a ocorrência dos crimes cibernéticos, com a adoção de legislação apropriada e pela promoção da cooperação internacional, entre outras medidas cabíveis.

Não pode deixar de destacar o Tratado da Organização das Nações Unidas (ONU) contra crimes cibernéticos no mundo, que foi assinado por 65 (sessenta e cinco) países e o Brasil foi um deles, a assinatura ocorreu no Vietnã na data de 25/10/2025. Durante o momento da assinatura, foi destacado que “o cibercrime é um problema real em todo o mundo” e que “todos estão lidando com isso”, evidenciando a dimensão global dessa ameaça, assim sendo, com esse tratado o País e mundo terá discussões com mais frequências voltadas ao combate ao cibercrime. Apesar das críticas de empresas de tecnologia e organizações de direitos humanos, que temem um possível aumento da vigilância estatal, o Brasil aderiu ao acordo, com a assinatura realizada pelo diretor-geral da Polícia Federal, Andrei Rodrigues.

O Tratado é visto pelo líder da ONU como uma resposta direta ao avanço e à complexidade dos delitos virtuais, representando um instrumento jurídico robusto e vinculativo capaz de fortalecer a proteção coletiva e impedir que ninguém esteja desprotegido contra os crimes digitais. No tocante, entre as inovações mais relevantes, destaca-se o mecanismo de compartilhamento de provas digitais entre diferentes países, superando um dos maiores entraves à efetividade da justiça no ambiente cibernético. E conforme ressaltado na reunião, pela primeira vez os investigadores passam a contar com um caminho claro para atuar em investigações transnacionais, mesmo quando o criminoso se encontrar em um país, a vítima em outro e as evidências em um terceiro, ampliando significativamente a eficiência e a cooperação internacional no combate ao cibercrime.

Em suma, esse documento surge como um marco essencial ao reforçar a segurança digital no mundo e assegurar a proteção dos direitos humanos no meio on-line. Ele representa um compromisso internacional que irá criar estratégias sólidas para o amparo às vítimas e garantir que as liberdades e garantias fundamentais sejam preservadas tanto no mundo físico quanto no virtual. Trata-se, portanto, de uma iniciativa que busca equilibrar o avanço tecnológico, responsabilidade estatal e defesa da dignidade humana em todas as dimensões da vida contemporânea.

8 PROCEDIMENTOS METODOLÓGICOS

Na presente pesquisa foi adotada a metodologia fundamentada em uma abordagem qualitativa, por possibilitar a compreensão aprofundada dos fenômenos sociais, psicológicos e jurídicos envolvidos nos crimes cibernéticos, especialmente no que se refere aos desafios da investigação forense digital e à violação dos direitos humanos no meio digital. No tocante, tratando-se de um assunto complexo, dinâmico e em constante evolução tecnológica, a abordagem qualitativa mostra-se a mais adequada para analisar não apenas aspectos legais, mas também os impactos sociais e emocionais decorrentes das práticas dos delitos virtuais. Sendo notável a complementação quantitativa a partir da análise de dados estatísticos oficiais relativos à ocorrência de crimes cibernéticos no Brasil.

O estudo caracteriza-se como pesquisa bibliográfica e documental, construído a partir da análise de legislações nacionais e internacionais (como a Constituição Federal, o Código Penal, a Lei 737/2012, a Lei 14.155/2021, o Marco Civil da *Internet*, a LGPD, Projeto de Lei n.º 4.658/2024, a Convenção de *Budapeste* de 2023 e o Tratado Global sobre Cibercrime da ONU), além de artigos científicos disponibilizados pelo *Scielo* Brasil e Google Acadêmico, revistas científicas, doutrinas atuais (livro físico), bem como, foram utilizadas informações concretas de órgãos como o CNJ, Polícia Civil, Delegacias de crimes cibernéticos, DataSenado, e pesquisas contemporâneas sobre cybercrime e perícia forense.

Destarte, foi empregada também a abordagem descritiva, por buscar expor, com precisão, as modalidades de crimes cibernéticos, suas características, os impactos psicológicos sofridos pelas vítimas, as fragilidades dos sistemas investigativo brasileiro e as limitações estruturais enfrentadas pelos peritos forenses. O método de raciocínio usado é o dedutivo, partindo de conceitos gerais sobre a evolução digital, a natureza dos cibercrimes e as garantias constitucionais, para então analisar questões específicas, como a atuação dos peritos, os desafios investigativos e as lacunas legais ainda encontradas que dificultam a responsabilização dos criminosos. Em suma, o levantamento teórico mostrou que a perícia forense digital enfrenta consideravelmente a falta de profissionais, poucos

investimentos, crescente demanda de crimes, que exige técnicas altamente sofisticadas e específicas todos os dias, para garantir a eficácia das investigações forenses.

9 ANÁLISE DOS RESULTADOS

A pesquisa demonstra que o enfrentamento dos crimes cibernéticos no Brasil ainda é marcado por avanços legais pontuais, mas severas deficiências estruturais e operacionais. Embora leis como a de n.º 12.737/2012 e n.º 14.155/2021 representem marcos relevantes, persiste um descompasso entre o texto normativo e sua efetiva aplicação, evidenciando a ausência de uma política pública contínua de cibersegurança. Os resultados indicam a necessidade de uma legislação mais ampla e específica, capaz de tipificar integralmente os delitos digitais e de estabelecer penas mais severas condizentes com a gravidade e o impacto social dessas condutas. Atinente a isso, foi possível verificar também que a Ciência Forense Digital, embora essencial para as investigações, enfrenta limitações relacionadas à falta de infraestrutura, investimento de equipamentos, profissionais qualificados e desafios éticos e técnicos, fatores que comprometem a devida coleta e validade de provas criminais.

Além disso, o estudo evidenciou o profundo impacto psicológico e social causados às vítimas, reforçando a urgência de políticas integradas de prevenção, embate e acolhimento. No contexto internacional, a adesão plena à Convenção de *Budapeste*, o avanço do Projeto de Lei n.º 4.658/2024 e o Tratado da ONU, surgem como medidas estratégicas para o fortalecimento da cooperação global para a minimização dos cybercrimes.

No tocante ao tema que é uma problemática atual, mesmo com a existência de importantes instrumentos legais no País, torna-se imprescindível que haja a aplicabilidade dessas leis, a abordagem interdisciplinar que una tecnologia, preparo e proteção à dignidade humana e a ampla divulgação, de modo que a população tenha a devida consciência de seus direitos e deveres no berço social digital.

10 CONSIDERAÇÕES FINAIS

Diante do exposto, observa-se que os crimes cibernéticos representam uma das maiores ameaças à segurança e à dignidade humana na era digital. A pesquisa buscou demonstrar a relevância da investigação forense no meio digital como instrumento indispensável à identificação, apuração e responsabilização dos crimes e dos perfis criminosos de delitos virtuais, bem como evidenciar os desafios enfrentados nesse campo, especialmente no Brasil. Contudo, permanece evidente que o País ainda enfrenta significativos desafios na área forense digital, como a escassez de profissionais

capacitados, a falta de investimentos em equipamentos próprios para as investigações compatível com a crescente complexidade dos delitos virtuais, que vem aumentando dia após dia.

Dessarte, ficou evidente que, para minimizar essa problemática, é imprescindível a ampliação da conscientização social, iniciando-se desde a base escolar, de modo que crianças e jovens compreendam o contexto dos crimes cibernéticos, suas consequências e as formas de prevenção. Além disso, é necessário o aperfeiçoamento legislativo, com maior tipificação e rigor na punição, a fim de garantir respostas mais eficazes e justas, à semelhança do agravamento previsto para crimes contra a honra cometidos no ambiente digital. Sendo plausível também, reforçar a urgência de políticas públicas eficazes, tanto para prevenção quanto para o acolhimento das vítimas que muitas das vezes sofrem caladas, assegurando a proteção de direitos fundamentais como a intimidade, honra e dignidade

Em suma, o perito forense digital desempenha papel essencial na promoção da segurança, na defesa dos direitos humanos no ciberespaço e no fortalecimento da justiça diante dos desafios impostos pelo berço digital contemporâneo. Atinente a isso, o Estado precisa dar mais atenção a esse assunto, proporcionando mais oportunidades de peritos em TI e por meio das mídias sociais e da educação promover maior viabilidade da relevância do cuidado, proteção e controle da ocorrência dos cibercrimes.

Por fim, o estudo evidencia, portanto, a urgência de políticas públicas voltadas à educação digital, à capacitação técnica dos profissionais e ao fortalecimento das estruturas de cibersegurança e perícia forense. Somente com a união entre conhecimento, ética e inovação será possível reduzir a incidência desses delitos e assegurar um ambiente virtual mais seguro, responsável e humanizado.

Assim, finaliza-se com as palavras de Pinheiro (2023), que diz que o Direito Digital traz uma necessidade de atualização tecnológica não só para advogados e juízes, como para delegados, procuradores, investigadores, peritos e todos os demais. Esta mudança de postura é importante para que se possa ter uma sociedade digital segura; contrário a isso, coloca-se em risco o próprio ordenamento jurídico.

REFERÊNCIAS

ALEXANDRE, Brenda C.; ARAÚJO, Giulianna M. A evolução dos crimes cibernéticos e os desafios da legislação brasileira. **RevistaFT**, Rio de Janeiro, v. 27, 2023. Disponível em: https://revistaft.com.br/a-evolucao-dos-crimes-ciberneticos-e-os-desafios-da-legislacao-brasileira/. Acesso em: 25 out. 2025.

ANDRADE, Ingrid Lima de. Forense digital aplicada ao combate de crimes cibernéticos: uma revisão. **Revista foco**, Minas Gerais, v. 17, n. 7, p. 01-27, 2024. Disponível em: https://ojs.focopublicacoes.com.br/foco/article/view/5771. Acesso em: 14 abr. 2025.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, [2016]. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/ Constituicao.htm. Acesso em: 14 abr. 2025.

BRASIL. **Decreto nº 11.491, de 12 de abril de 2023**. Promulga a convenção sobre o crime cibernético, firmada pela república federativa do brasil, em budapeste, em 23 de novembro de 2001. Brasília, DF: Presidência da República, 13 abr. 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11491.htm. Acesso em: 25 out. 2025.

BRASIL. **Decreto-Lei n.º 2.848, de 7 de dezembro de 1940**. Código penal. Rio de Janeiro, RJ: Presidência da República, 31 dez. 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 13 nov. 2025.

BRASIL. **Lei n. º 13.709, de 14 de agosto de 2018**. Lei geral de proteção de dados pessoais (lgpd). Brasília, DF: Presidência da República, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 13 nov. 2025.

BRASIL. **Lei n.º 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o decreto-Lei nº 2.848, de 7 de dezembro de 1940 - código penal; e dá outras providências. Brasília, DF: Presidência da República, 3 dez. 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 13 nov. 2025.

BRASIL. **Lei n.º 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da internet no brasil. Brasília, DF: Presidência da República, 24 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 13 nov. 2025.

BRASIL. **Lei n.º 14.155, de 27 de maio de 2021**. Altera o decreto-lei nº 2.848, de 7 de dezembro de 1940 (código penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o decreto-lei nº 3.689, de 3 de outubro de 1941 (código de processo penal), para definir a competência em modalidades de estelionato. Brasília, DF: Presidência da República, 28 mai. 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm. Acesso em: 25 out. 2025.

CADILHAC, Tálita. **Os crimes cibernéticos e o trabalho do perito forense computacional: práticas de investigação criminal computacional**. 2022. Trabalho de Conclusão de Curso - TCC (Graduação em Direito) – Faculdade de Direito, Centro Universitário Sociesc de Blumenau – UNISOCIESC, Blumenau, 2022.

CALGAROTO, Cléber. **O direito à privacidade na internet: panorama, responsabilização civil e inovações do marco civil da internet (lei nº 12.965/2014)**. 2021. Monografia (Graduação em Direito) – Faculdade de Direito, Universidade do Sul de Santa Catarina, Palhoça, 2021.

CÂMARA, Agência. **Conheça a evolução dos crimes cibernéticos**. *Câmara dos Deputados*, 2006. Disponível em: https://www.camara.leg.br/noticias/89137-conheca-a-evolucao-dos-crimes-ciberneticos. Acesso em: 25 out. 2025.
CHURCH, Life. **Isaías 61:8**. *YouVersion*, 2025. Disponível em: https://www.bible.com/pt/bible/compare/ISA.61.8. Acesso em: 14 nov. 2025.

COSTA, Emanuely S.; SILVA, Raíla C da. Crimes cibernéticos e investigação policial. **Revista eletrônica do ministério público do estado do piauí**, Piauí, p. 181-196, 2021. Disponível em: https://www.mppi.mp.br/internet/wp-content/uploads/2022/06/Crimes-ciberne%CC%81ticos-e-investigac%CC%A7a%CC%83o-policial.pdf. Acesso em: 14 abr. 2025.

DEPUTADOS, Câmara dos. **Projeto de lei n.º 4.658, de 2024**. Altera o decreto-lei 2.848, de 1940 - código penal. para estabelecer tratamento penal majorado aos crimes praticados por meios digitais. Brasília – DF: Congresso Nacional, 2024. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2862637&filename=Avulso%20PL%204658/2024. Acesso em: 16 nov. 2025.

DOMINGOS, Thaís G.; JACOB, Alexandre. O perfil do criminoso nos crimes cibernéticos: comportamentos, motivações e táticas. **Revista multidisciplinar do nordeste mineiro**, Minas Gerais, v.10, n. 1, p. 1-13, 2024. Disponível em: https://remunom.ojsbr.com/multidisciplinar/article/view/2980. Acesso em: 25 out. 2025.

ESCOLA, Brasil. **Internet no brasil**. *Brasil Escola*. Disponível em: https://brasilescola.uol.com.br/informatica/internet-no-brasil.htm. Acesso em: 13 nov. 2025.

GOLPES de clonagem de voz avançam com uso de inteligência artificial. Direção: Carolina Ferraz, Roberto Cabrini, Entrevistados: Delegado Paulo Eduardo, Dario Centurione, Fernando Ferreira, Delegado Pablo Sartori, Entrevistador: Pedro Paulo, 12 out. 2025. 1 vídeo (8:08.). Publicado pelo canal Domingo Espetacular. Disponível em: https://www.youtube.com/watch?v=vqx5DiIuVUQ. Acesso em: 11 nov. 2025.

JUSTIÇA, Superior Tribunal de. **Crime cibernético tomou lugar de roubos e furtos na pandemia, diz ministro humberto martins**. *STJ Superior Tribunal de Justiça*, 2020. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/Crime-cibernetico-tomou-lugar-de-roubos-e-furtos-na-pandemia--diz-o-ministro-Humberto-Martins.aspx. Acesso em: 13 nov. 2025.

KOETZ, Eduardo. **Cibercrime: entenda o que é, quais são os tipos e como prevenir**. *ADVBOX*| *Blog*, 2024. Disponível em: https://advbox.com.br/blog/cibercrime/. Acesso em: 13 nov. 2025.

LEITE, Fredson Gustavo de Souza *et al.* **Crimes cibernéticos: fraude eletrônica e a efetividade da legislação brasileira**. 2025. Trabalho de Conclusão de Curso – TCC (Graduação em Direito) -Faculdade de Direito, Centro Universitário Aparício Carvalho – FIMCA, Porto Velho, 2025.

LIMA, Douglas Magno Fernandes do Nascimento. **Os desafios da investigação nos crimes cibernéticos**. 2024. Trabalho de Conclusão de Curso – TCC (Graduação em Direito) – Faculdade de Direito, Universidade Federal da Paraíba (UFPB), Santa Rita, 2024.

MAIA, Karolline B.; COSTA, Cezar H F. Crimes cibernéticos. **Revista ibero-americana de humanidades, ciências e educação - rease**, São Paulo, v. 9, n. 10, p. 109–126, 2023. Disponível em: https://periodicorease.pro.br/rease/article/view/11580. Acesso em: 11 nov. 2025.

MELO, Luiza. **Golpes virtuais aumentam e não fazem distinção de idade**. *senadonotícias*, 2025. Disponível em: https://www12.senado.leg.br/noticias/infomaterias/2025/04/golpes-virtuais-aumentam-e-nao-fazem-distincao-de-idade. Acesso em: 13 nov. 2025.

NAKAMURA, João. **Brasil é vice-campeão em ataques cibernéticos, com 1.379 golpes por minuto, aponta estudo**. *CNN BRASIL*, 2024. Disponível em: https://www.cnnbrasil.com.br/economia/negocios/brasil-e-vice-campeao-em-ataques-ciberneticos-com-1-379-golpes-por-minuto-aponta-estudo/. Acesso em: 13 nov. 2025.

NOTÍCIAS, Agência Câmara. **Projeto aumenta pena para crimes praticados no meio digital.** *Câmara dos Deputados,* 2025. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2474869. Acesso em: 25 out. 2025.

O QUE é o Marco Civil da Internet? | *desinformante explica. Gravado pelo jornalista e pesquisador Rodolfo Viana, 2 de ago. de 2023. 1 vídeo (5:05.). Publicado pelo canal *desinformante. Disponível em: https://www.youtube.com/watch?v=L0mKvO27n_g. Acesso em: 13 nov. 2025.

OLIVEIRA, Geovana Xavier de. **Crimes cibernéticos: direito digital e os novos paradigmas da investigação criminal**. 2022. Artigo Científico (Graduação em Direito) – Faculdade de Direito, Pontifícia Universidade Católica de Goiás, Goiânia, 2022.

PADILHA, Rafael *et al.* A inteligência artificial e os desafios da ciência forense digital no século XXI. **Estudos Avançados**, Campinas, v. 35, n. 101, p. 111–138, 2021. Disponível em: https://revistas.usp.br/eav/article/view/185039. Acesso em: 10 nov. 2025.

PINHEIRO, Patrícia. **#Direitodigital.** 7. ed. São Paulo, 2023.

PRESSE, France. **Mais de 60 países, incluindo o brasil, assinam tratado da onu contra cibercrime criticado por ongs**. *g1*, 2025. Disponível em: https://g1.globo.com/mundo/noticia/2025/10/25/mais-de-60-paises-incluindo-o-brasil-assinam-tratado-da-onu-contra-cibercrime-criticado-por-ongs.ghtml. Acesso em: 13 nov. 2025.

QUEIROZ, Liv F A S. Os crimes cibernéticos no ordenamento jurídico brasileiro: investigação criminal e desafios. **Revista do CNMP**, n. 12, p. 417–448, 2025. Disponível em: https://ojs.cnmp.mp.br/index.php/revistacnmp/article/view/707. Acesso em: 11 nov. 2025
SANTOS, Orismar Teixeira dos.; NUNES, Nathalia Pereira. **Evolução dos crimes cibernéticos na pandemia**. 2023. Trabalho de Conclusão de Curso – TCC (Graduação em Administração) – Faculdade de Administração, Universidade Federal de Mato Grosso do Sul, Mato Grosso do Sul, 2023.

SILVA, Silene Tomaz da. **Crimes cibernéticos**. 2018. Trabalho de Conclusão de Curso - TCC (Graduação em Direito) - Faculdade de Direito, Universidade de Cuiabá /UNIC/IUNI, Cuiabá, 2018.

TARSO, David de. **Polícia esclarece maior ataque hacker do país e prende envolvido em desvio de R$ 541 milhões**. *JP Grupo Jovem Pan*, 2025. Disponível em: https://jovempan.com.br/opiniao-jovem-pan/comentaristas/david-de-tarso/policia-esclarece-maior-ataque-hacker-do-pais-e-prende-envolvido-em-desvio-de-r-541-milhoes.html. Acesso em: 11 nov. 2025.

TELECOMUNICAÇÕES, Agência Nacional de. **Portaria nº 148, de 31 de maio de 1995**. Aprova a norma nº 004/95 - uso da rede pública de telecomunicações para acesso à internet.1 jun. 1995.

Disponível em: https://informacoes.anatel.gov.br/legislacao/normas-do-mc/78-portaria-148. Acesso em: 13 nov. 2025.

UNIDAS, Nações. **Líder da onu participa de assinatura da tratado sobre crime cibernético, em hanói**. *ONU News Perspectiva Global Reportagens Humanas*, 2025. Disponível em: https://news.un.org/pt/story/2025/10/1851341. Acesso em: 11 nov. 2025.

unifaema Biblioteca Júlio Bordignon

RELATÓRIO DE VERIFICAÇÃO DE PLÁGIO

DISCENTE: Thaís Giega de Souza

CURSO: Direito

DATA DE ANÁLISE: 17.11.2025

RESULTADO DA ANÁLISE

Estatísticas

Suspeitas na Internet: **3,01%**
Percentual do texto com expressões localizadas na internet ⚠

Suspeitas confirmadas: **2,65%**
Confirmada existência dos trechos suspeitos nos endereços encontrados ⚠

Texto analisado: **96,99%**
Percentual do texto efetivamente analisado (frases curtas, caracteres especiais, texto quebrado não são analisados).

Sucesso da análise: **100%**
Percentual das pesquisas com sucesso, indica a qualidade da análise, quanto maior, melhor.

Analisado por Plagius - Detector de Plágio 2.9.6
segunda-feira, 17 de novembro de 2025

PARECER FINAL

Declaro para devidos fins, que o trabalho da discente THAÍS GIEGA DE SOUZA n. de matrícula **36784,** do curso de Direito, foi aprovado na verificação de plágio, com porcentagem conferida em 3,01%. Devendo a aluna realizar as correções necessárias.

Assinado digitalmente por: ISABELLE DA SILVA SOUZA
Razão: Responsável pelo documento
Localização: UNIFAEMA - Ariqueme/RO
O tempo: 17-11-2025 14:20:54

ISABELLE DA SILVA SOUZA
Bibliotecária CRB 1148/11
Biblioteca Central Júlio Bordignon
Centro Universitário Faema – UNIFAEMA