UNILEÃO
CENTRO UNIVERSITÁRIO DOUTOR LEÃO SAMPAIO
CURSO DE GRADUAÇÃO EM DIREITO

LAIS RODRIGUES TELES

CRIMES CIBERNÉTICOS NO DIREITO BRASILEIRO:evolução legislativa e desafios práticos

JUAZEIRO DO NORTE-CE
2025

LAIS RODRIGUES TELES

CRIMES CIBERNÉTICOS NO DIREITO BRASILEIRO:evolução legislativa e desafios práticos

Projeto apresentado ao Centro Universitário Doutor Leão Sampaio/UniLeão, como requisito para a obtenção de nota da disciplina Metodologia da Pesquisa, sob orientação da Prof. Alyne Leite de Oliveira.
Professor Orientador da Pesquisa: Francisco Gledison Lima Araujo.

JUAZEIRO DO NORTE-CE
2025

LAIS RODRIGUES TELES

TIPIFICAÇÃO DOS CRIMES CIBERNÉTICOS NO DIREITO BRASILEIRO:evolução legislativa e desafios práticos

Este exemplar corresponde à redação final aprovada do Trabalho de Conclusão de Curso de LAIS RODRIGUES TELES.

Data da Apresentação __20_/_06__/_2025___

BANCA EXAMINADORA

Orientador: Professor Francisco Gledison Lima Araujo

Membro: Professor André Carvalho Barreto / Unileão

Membro: Professor Francisco Thiago Da Silva Mendes / Unileão

JUAZEIRO DO NORTE-CE
2025

TIPIFICAÇÃO DOS CRIMES CIBERNÉTICOS NO DIREITO BRASILEIRO:evolução legislativa e desafios práticos

Lais Rodrigues Teles[1]
Francisco Gledison Lima Araujo[2]

RESUMO

O presente estudo busca analisar o panorama histórico, normativo e prático do cibercrime no Brasil, assim como a evolução da legislação brasileira diante dos avanços tecnológicos e do aumento dos crimes cibernéticos, investigando se o atual arcabouço jurídico é suficiente para garantir proteção, segurança e direitos no ambiente digital, a fim de contribuir para o aprimoramento de políticas públicas e fortalecer a investigação e punição desses crimes. Para tanto, o artigo analisa a evolução histórica da internet e dos crimes cibernéticos, assim como as principais leis brasileiras relacionadas. A metodologia do estudo foi baseada em uma pesquisa bibliográfica qualitativa e exploratória, que envolveu a análise crítica de documentos jurídicos, artigos científicos e jurisprudências recentes. O texto aborda a evolução do direito digital e argumenta que o Direito Cibernético desempenha papel crucial na adaptação das normas jurídicas às novas realidades tecnológicas. Explora os desafios enfrentados na investigação desses crimes e conclui que é fundamental fundir conhecimentos do mundo digital ao direito assim como continuar adaptando o Direito brasileiro às constantes mudanças tecnológicas e sociais. O estudo identificou que, embora o Brasil tenha avançado na criação de leis específicas para o combate aos crimes cibernéticos, existem fragilidades na aplicação prática dessas normas devido à constante inovação tecnológica. Além disso, ressaltou a importância da cooperação internacional, padronização dos procedimentos legais e a necessidade de harmonização legislativa. O fortalecimento institucional e a capacitação técnica foram apontados como essenciais para aprimorar a eficácia no combate aos crimes digitais.

Palavras-Chave: Cibercrime; Ordenamento jurídico; Tipificação; Condutas.

1 INTRODUÇÃO

Nas últimas décadas, a incidência de crimes cibernéticos no Brasil cresceu de forma exponencial, acompanhando a rápida digitalização da sociedade e a ampliação do acesso à internet. Esse fenômeno trouxe não apenas benefícios, como maior conectividade e inovação, mas também desafios inéditos para a segurança pública e para o ordenamento jurídico. A facilidade de acesso a dados, a sofisticação dos ataques e a transnacionalidade das condutas ilícitas evidenciam a necessidade de uma análise crítica sobre a eficácia da legislação penal vigente frente à complexidade e à dinamicidade dos delitos digitais.

Nesse contexto, o presente artigo tem como objetivo central examinar a tipificação dos crimes cibernéticos no direito brasileiro, avaliando a efetividade das normas atualmente em vigor. A problemática reside na defasagem entre a evolução tecnológica e a atualização do

[1] Lais Rodrigues Teles Graduanda do Curso de Direito do Centro Universitário Doutor Leão Sampaio/Unileão-lalirt314@gmail.com.

[2] Prof. Francisco Gledison Lima Araujo, Mestrando em Direito Constitucional pela UNIFIEO-SP, Especialista em DIreito DIgital - CEDIN-MG, Especialista em Direito Público - Legale-SP,gldaraujo@gmail.com.

arcabouço jurídico, o que pode resultar em lacunas normativas e dificultar a responsabilização dos agentes. Justifica-se a pesquisa pela urgência em compreender se o aparato legal brasileiro é suficiente para enfrentar as novas modalidades de crime, protegendo os direitos dos cidadãos e garantindo a segurança no ambiente digital.

A hipótese que norteia este estudo é que, embora o Brasil tenha avançado na promulgação de leis específicas para o combate aos crimes cibernéticos, como a Lei nº 12.737/2012 (Lei Carolina Dieckmann) e a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), ainda existem fragilidades na aplicação prática dessas normas diante da constante inovação tecnológica. Assim, questiona-se: a legislação penal brasileira está preparada para acompanhar a evolução dos delitos cibernéticos e assegurar uma resposta eficaz a essas ameaças?

Para responder a essa questão, o artigo propõe, como objetivo especifico, uma análise abrangente do crescimento dos crimes virtuais no Brasil, bem como da evolução legislativa destinada ao seu enfrentamento. Foram destacados, na mesma estrutura, os principais marcos normativos e discutidas as necessidades de adaptações legislativas, visando garantir a proteção dos direitos fundamentais e a efetividade das respostas penais diante de um cenário digital em permanente transformação.

A relevância deste debate é reforçada ao abordar a evolução histórica da legislação nacional, os desafios práticos na investigação e responsabilização dos crimes digitais, e a necessidade de constante atualização normativa.

2 DESENVOLVIMENTO

O presente estudo busca examinar o panorama histórico, normativo e pratico do cibercrime no Brasil, assim como a evolução da legislação brasileira diante dos avanços tecnológicos e do aumento dos crimes cibernéticos, investigando se o atual arcabouço jurídico é suficiente para garantir proteção, segurança e direitos no ambiente digital, bem como contribuir para o aprimoramento de políticas públicas e fortalecer a investigação e punição desses crimes, colaborando para um ambiente virtual mais seguro e justo. Para isso, foram abordados conceitos fundamentais, a evolução histórica dos cibercrimes assim como o trabalho de diversos autores, através do método de analise interpretativa e pesquisa qualitativa.

O estudo apresenta capítulos que contextualizam historicamente a internet no Brasil, discutem a sociedade da informação, analisam a internet como ferramenta para cibercrimes,

abordam estratégias de combate a esses delitos e examinam os desafios da tipificação dos cibercrimes no país.

2.1 METODOLOGIA

A pesquisa foi conduzida por meio de revisão bibliográfica, com base na análise de documentos jurídicos, trabalhos de diversos autores, artigos científicos e jurisprudências recentes, alem de leis como: a Lei Geral de Proteção de Dados (LGPD), Lei nº 12.965/2014 (Marco Civil da Internet) e Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann. A metodologia adotada é de caráter qualitativo e exploratório.

Na medida em que explora o crescimento da legislação diante dos avanços tecnológicos, garantindo proteção jurídica, segurança e direitos no ambiente digital. Além disso, contribui para o aprimoramento de políticas públicas, fortalecendo a investigação e punição desses crimes, colaborando para um ambiente virtual mais seguro e justo para todos.

Para alcançar o objetivo proposto, esta pesquisa foi conduzida mediante uma abordagem baseada em pesquisa bibliográfica. A pesquisa bibliográfica é um método amplamente reconhecido e utilizado na academia, que envolve a busca e análise crítica de fontes bibliográficas, incluindo livros, artigos científicos, legislação, jurisprudência e documentos governamentais relacionados ao tema em questão. Essa metodologia permitiu uma investigação aprofundada da evolução da legislação penal no contexto dos crimes cibernéticos.

2.2 REFERENCIAL TEÓRICO

2.2.1 Análise Histórica da Internet no Brasil

Segundo pesquisas da Revista Pesquisa Fapesp (2011) e do Laboratório Nacional de Computação – LNCC (2022), a internet no Brasil teve seu início em 1988, quando a Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP) e o Laboratório Nacional de Computação Científica (LNCC) estabeleceram conexões com instituições nos Estados Unidos através da Bitnet. Em 1989, a Rede Nacional de Pesquisa (RNP) foi criada para coordenar o acesso à internet no país.

Durante a década de 1990, a RNP expandiu o acesso à internet para cerca de 600 instituições, atingindo aproximadamente 65 mil usuários. Em 1995, a internet começou a ser

explorada comercialmente no Brasil. Nos anos seguintes, a internet se popularizou com o surgimento de provedores de acesso e a expansão da banda larga. Em 2004, as redes sociais começaram a se destacar, e em 2007, a conexão móvel se tornou mais acessível. Hoje, a internet é necessária para a sociedade brasileira, com mais de 50% dos domicílios conectados desde 2016.

Segundo informa o Instituto de Pesquisa Econômica Aplicada – IPEA (2023) e o Instituto Brasileiro de Geografia e Estatística – IBGE (2020), a pandemia de Covid-19 acelerou ainda mais a demanda por serviços online no país. O mundo digital passou a desempenhar um papel importante na economia e sociedade, tornando-se necessario para a manutenção do mercado de trabalho, ambiente educacional e ate procedimentos legais, trazendo grandes avanços no campo das interações remotas e desenvolvimento de inteligências artificiais; mas também trouxe desafios significativos.

O aumento dos crimes cibernéticos foi impulsionado pela maior dependência da internet e do trabalho remoto, permitindo que cibercriminosos explorassem as vulnerabilidades das infraestruturas digitais. Além disso, a adoção acelerada do trabalho remoto criou novos vetores de ataque, enquanto a desinformação e os golpes online se proliferaram, explorando o medo e a incerteza generalizados. As dificuldades na segurança cibernética, especialmente em empresas mal preparadas, tornaram mais complexo o combate aos cibercrimes.

Tal situação criou um ambiente propício para o crescimento do cibercrime. Segundo relatórios feitos pela INTERPOL - Organização Internacional de Polícia Criminal (International Criminal Police Organization) em 2020, novos tipos de ataques cibernéticos, como phishing e ransomware, aumentaram drasticamente, explorando a ansiedade e a necessidade de informações durante a crise, também exacerbando o aumentando a vulnerabilidade de populações mais suscetíveis a crimes online.

> A cibercultura nada mais é do que a cultura contemporânea em sua interface com as novas tecnologias de comunicação e informação, ela está ligada às diversas influencias que estas tecnologias exercem sobre as formas de sociabilidade contemporâneas, influenciando o trabalho, a educação, o lazer, o comércio, etc. Todas as áreas da cultura contemporânea estão sendo reconfiguradas com a emergência da cibercultura (Lemos, 2003; p. 1).

Consequentemente, esse comportamento inovador e singular introduz uma nova modalidade de cultura predatória, que, impulsionada por diversas inovações, utiliza estas ferramentas como meio criminal e artefacto lesivo.

O uso criativo e estratégico de recursos digitais para práticas criminosas demonstra a necessidade de constante atualização das leis e de mecanismos de fiscalização, a fim de

acompanhar as transformações e proteger a sociedade dos riscos emergentes associados à cultura digital predatória.

2.2.2 Cooperação Internacional no Combate aos Crimes Cibernéticos: Desafios e Avanços no Brasil

A cooperação internacional é um elemento fundamental no combate aos crimes cibernéticos, dada a natureza transnacional dessas infrações e a facilidade com que criminosos podem operar a partir de diferentes jurisdições. No contexto brasileiro, o Brasil se tornou oficialmente signatário da Convenção sobre o Crime Cibernético com a promulgação do Decreto nº 11.491, assinado pelo Vice-Presidente da República no exercício da Presidência, em 12 de abril de 2023, formalizando a adesão ao tratado firmado em Budapeste em 2001, como anuncia o IBDFAM – Instituto Brasileiro do Direito de Familia (2023). Essa adesão representa um passo importante para alinhar os procedimentos de investigação e repressão a padrões globais. Países que já implementaram a Convenção conseguiram aprimorar a troca de informações e agilizar a obtenção de provas digitais, ao seguirem os protocolos apresentados no texto desta, o que se traduz em maior eficiência na identificação e responsabilização de criminosos.

Um exemplo positivo de cooperação internacional pode ser observado nas operações conjuntas entre a Polícia Federal brasileira e agências internacionais, através do uso da Rede de Cooperação Internacional em Crimes Cibernéticos, criada em 2023, para fortalecer a cooperação policial internacional, o que já resultou em diversas operações bem-sucedidas, impulsionando o combate de crimes como a fraude cibernetica, o tráfico de drogas, o furto criptoativo e ate o abuso sexual infantojuvenil, entre outros, como se pode observar com as notícias publicadas no site do Ministério da Justiça e Segurança Pública – MJSP (2025). A atuação conjunta permitiu a identificação de vítimas e a prisão de criminosos, demonstrando que a colaboração transnacional pode gerar resultados concretos e proteger a população de crimes digitais graves. Entretanto, o Brasil ainda enfrenta desafios para aderir plenamente ao tratado, principalmente devido à necessidade de adequação legislativa e à preocupação com a soberania nacional.

Persistem, deste modo, desafios significativos para a efetiva implementação da cooperação internacional no Brasil. Um dos principais obstáculos é a falta de padronização dos procedimentos legais, o que dificulta a execução de pedidos de cooperação jurídica internacional e pode atrasar investigações sensíveis. Além disso, a burocracia e a morosidade

no trâmite de cartas rogatórias e acordos de assistência mútua prejudicam a agilidade necessária para combater crimes digitais, que frequentemente exigem respostas em tempo real. Essas dificuldades são agravadas pela carência de recursos humanos especializados e pela limitação tecnológica de muitos órgãos públicos brasileiros, destaca o trabalho de Guidi e Rezek (2023) na Revista Brasileira de Política Pública.

Outro desafio relevante se trata da proteção de dados e à privacidade dos cidadãos brasileiros durante o intercâmbio internacional de informações. A ausência de uma legislação harmonizada com os principais parceiros internacionais pode gerar conflitos normativos, especialmente em relação à transferência de dados pessoais para países que não oferecem o mesmo nível de proteção previsto na Lei Geral de Proteção de Dados (LGPD). Esse cenário pode limitar a cooperação com países da União Europeia, por exemplo, e dificultar investigações de crimes que envolvam múltiplas jurisdições, apoia Belli et al. (2024).

Por fim, é importante destacar que, ainda com base no trabalho de Belli et al. (2024), a efetividade da cooperação internacional depende também do fortalecimento das capacidades institucionais brasileiras. Investir em capacitação técnica, atualização de equipamentos e integração de bancos de dados são medidas essenciais para que o Brasil possa atuar de forma proativa e alinhada com os padrões internacionais. Além disso, a criação de unidades especializadas em cibercrimes e a participação ativa em fóruns multilaterais contribuem para o desenvolvimento de boas práticas e para a construção de uma rede global de combate ao cibercrime. Superar os desafios existentes e consolidar os bons resultados já obtidos passa, portanto, por um compromisso contínuo com a modernização institucional e a articulação internacional.

2.2.3 A Sociedade da Informação

A sociedade da informação não representa apenas um avanço tecnológico, mas uma nova realidade cultural que exige regulamentações específicas para garantir direitos e deveres dos cidadãos no meio digital.

Como destaca Carvalho (2014) o ser humano contemporâneo vive em um contexto marcado pelo rápido avanço dos meios digitais, que não só modificaram os equipamentos tecnológicos e seu uso intenso, mas também influenciaram a maneira de pensar e agir das pessoas. Essa revolução digital resultou principalmente na rapidez e no dinamismo da disseminação de informações, permitindo o envio e o acesso a conteúdos atualizados a qualquer momento e de qualquer lugar com conexão à Internet.

Ainda mais, segundo avaliações internacionais da EUROPOL - Agência da União Europeia para a Cooperação Policial (2025), essa facilidade apresenta paralelamente múltiplos riscos, visto que os usuários deram início à exposição de maneira exacerbada de seus dados e informações na rede global de computadores, o que desperta o interesse de terceiros e agentes criminosos na busca por ganhos de forma clandestina.

Em sintonia com Borges:

> É certo que a criminalidade, obviamente, não deixaria de aproveitar as oportunidades trazidas pelas novas tecnologias, e a prática de ilícitos na Internet é uma realidade perversa, com um sem número de fraudes bancárias, extorsões decorrentes de invasões de computadores, vírus e programas espalhados pela rede para obtenção de dados que permitam a prática criminosa, pornografia infantil e muitas outras condutas ilícitas ou reprováveis (Borges, 2015; p. 1).

A rápida mudança nos hábitos eliminou as barreiras físicas e geográficas, permitindo que associações e negócios sejam estabelecidos com base em interesses comuns, graças às plataformas digitais que facilitam uma variedade de atividades no ciberespaço, criando uma sociedade diversa e constantemente conectada.

É fato que, neste contexto, o mau uso das ferramentas digitais tem um impacto significativo nas relações sociais e no ordenamento jurídico. A tendência atual e futura é migrar das ações físicas para as eletrónicas, tornando necessário reavaliar as normas legais sobre crimes virtuais para garantir maior segurança aos usuários no vasto espaço cibernético.

Discute Pinheiro (2021), que crimes virtuais são geralmente classificados em dois grandes grupos: aqueles cometidos diretamente contra sistemas de informática e aqueles que utilizam esses sistemas como meio para práticas ilícitas. Tais classificações englobam centenas de crimes digitais, para com os quais a jurimetria tem sido instrumento importante para a análise quantitativa de seus processos judiciais, permitindo compreender padrões e tendências legislativas a fim de efetivamente combatê-los, afinal, é fato que o cibercrime possui diversas denominações, variantes e subcategorias ainda não tipificadas.

Nas palavras de Augusto Rossini:

> O conceito de “delito informático” poderia ser talhado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade a confidencialidade (Rossini, 2004; p. 110).

No Brasil, surgiu a necessidade da criação de diversos aparatos jurídicos afim de regularizar, monitorar e proteger as interações no ciberespaço, estas adições ao código normativo representam marcos na regulamentação do ambiente digital.

Diante do presente cenário e das mudanças que este passou a exigir, e afim de

progredir o foco do presente estudo, faz-se valioso realizar uma breve análise histórica da Internet e sua disseminação no território nacional, com o propósito de dissecar a evolução e os efeitos jurídicos do cibercrime no Brasil

2.2.4 A Internet Como Ferramenta Para a Pratica de Cibercrimes

É simples notar o quanto o ser humano está interligado a tecnologia, bastando analisar sua rotina, na qual grande parte se desenrola nos ambientes eletrónicos. A internet, apesar de suas diversas vantagens, por ser ambiente amplo, tornou-se um ambiente propício para a prática de cibercrimes.

> Com o aparecimento da Internet como um novo instrumento de comunicação e o seu acesso cada vez mais presente em todas as classes sociais, profissionais e faixas etárias, relatos de comportamentos patológicos de dependência da Internet constituem temas frequentes da literatura médica atual e também, com grande destaque, na mídia popular (Razzouk, 1998; p. 1).

Como discute também, Pinheiro (2021), a dependência dos meios tecnológicos oferece mais oportunidades para os criminosos. Embora não seja uma "terra sem lei", o direito brasileiro ainda enfrenta desafios significativos, especialmente na materialidade dos delitos online.

Existem diversas formas pelas quais os delitos podem ocorrer no meio digital, incluindo invasão de sistemas, roubo de dados e falsidade ideológica, sendo que a identificação dos responsáveis é dificultada pelo anonimato proporcionado pela rede e pela limitada capacidade das autoridades brasileiras em rastrear esses criminosos. Embora a Internet ofereça inúmeros benefícios, ela também se torna um ambiente atrativo para criminosos, devido ao seu funcionamento complexo e interconectado, que muitos descrevem como um "caos organizado" onde tudo pode se conectar com apenas um clique, como destaca o trabalho de Costa (1998).

O fato é, como fica evidente atravez de relatórios apresentados pela EUROPOL (2025), estes delitos, podem ser cometidos por qualquer pessoa com acesso a internet, principalmente com o sentimento de segurança que vem do anonimato e com as diversas formas de mascarar endereços IP e criptografar dados, oferecidas por instrumentos prontamente disponíveis como VPNs e outros serviços intermediários entre usuário e rede.

Alem disto, a prática de cibercrimes tem se tornado cada vez mais sofisticada, incorporando tecnologias como inteligência artificial e *blockchain*, o que dificulta sua detecção e combate.

Nesse contexto de crescente complexidade tecnológica, a ausência de uma legislação específica e atualizada para o combate aos crimes cibernéticos torna-se um obstáculo significativo. A aplicação das normas penais tradicionais, como o Código Penal vigente, revela-se insuficiente para abranger todas as novas modalidades de delitos digitais, gerando lacunas jurídicas que podem resultar na impunidade dos responsáveis. Essa situação evidencia a urgência de uma normatização adequada que contemple as particularidades da informática no âmbito criminal.

Em relação ao tópico, afirma Teixeira:

> Há uma enorme expectativa e ansiedade para uma adequada normatização que trate da informática, especialmente no campo criminal, pois diante da ausência de legislação específica têm-se aplicado o Código Penal [...] Porém, outros delitos eventualmente podem não se enquadrar nos tipos penais estabelecidos até então, surgindo a denominada atipicidade do ato, com a consequente impunidade do agente criminoso (Teixeira, 2024; p. 623 à 637).

Essa lacuna normativa contribui para o aumento e a complexidade dos cibercrimes, pois dificulta a responsabilização efetiva dos infratores. Além disso, a facilidade de acesso a informações pessoais e sensíveis na internet potencializa a vulnerabilidade das vítimas, ampliando o campo de atuação dos criminosos digitais.

Como enfatiza, Deslandes e Arantes (2017), o aumento desses crimes está relacionado à facilidade de execução, uma vez que muitas informações pessoais estão disponíveis na internet, permitindo que criminosos coletem dados privilegiados para extorquir ou causar danos morais e financeiros às vítimas.

Para combater esses delitos, a cooperação entre governos e empresas é necessária para desenvolver leis e tecnologias que possam detectar, rastrear, identificar e tipificar estes crimes afim de corrigi-los de forma eficaz.

2.2.5 O Caminho Para Combater os Cibercrimes

A resposta ao cibercrime requer uma abordagem holística que combine estratégias políticas e tecnológicas. Neste contexto, a instituição de legislação e regulamentação eficazes faz-se necessaria para o combate efetivo de tal problemática. A criação de leis específicas é importante para estabelecer diretrizes sobre como lidar com com os, cada vez mais evoluídos, delitos digitais.

Silva (2003) destaca que o surgimento da informática na sociedade ocorreu de forma muito rápida, exigindo soluções imediatas que o Direito ainda não estava preparado para oferecer. Essa demanda social por regulamentação pode levar à criação excessiva de leis,

algumas desnecessárias, devido à busca urgente por proteção jurídica diante das transformações tecnológicas.

No mesmo contexto, Peck (2021), trata da necessidade de legislação específica para crimes cibernéticos e da importância de implementar políticas rigorosas de combate ao cibercrime, o que envolve o desenvolvimento e a aplicação de leis e regulamentos que tipifiquem as atividades cibernéticas maliciosas. No entanto, a utilização inadequada de técnicas e procedimentos informáticos pode gerar impactos significativos nas relações jurídicas, caso sejam empregados de maneira imprópria, por isso é importante incentivar a colaboração entre os setores público e privado para compartilhar informações sobre ameaças cibernéticas e desenvolver melhores práticas de segurança.

Investir em pesquisa e desenvolvimento de tecnologias de segurança avançadas, como inteligência artificial, pode fortalecer as defesas virtuais e ajudar a identificar e neutralizar possíveis ameaças de forma mais eficaz e contundente.

Afinal, como leciona Siqueira:

> Seria possível a identificação do criminoso obtendo o seu endereço de IP, login e senha do aparelho utilizado para a prática do crime, porém, os criminosos utilizam endereços falsos, dificultando o trabalho investigativo dos policiais (Siqueira, 2017; p. 122).

Além destas estratégias, seria importante que houvesse a criação de um órgão ou entidade com o propósito de monitorar e analisar continuamente as ameaças à segurança cibernética, sendo essencial uma abordagem coordenada e colaborativa entre as autoridades assim como o compartilhamento de recursos entre estas.

A implementação de um órgão especializado permitiria maior agilidade na identificação de novas ameaças e na resposta a incidentes, além de promover o intercâmbio de informações e boas práticas entre diferentes setores envolvidos na segurança digital. Essa estrutura também facilitaria a integração de esforços nacionais com iniciativas internacionais, fortalecendo a capacidade do país de prevenir e combater cibercrimes de forma mais eficaz e alinhada com os padrões globais de proteção cibernética.

2.2.6 Desafios e Lacunas da Legislação Brasileira Frente aos Crimes Cibernéticos e a Inteligência Artificial

A legislação brasileira enfrenta desafios crescentes na produção de normas e na classificação de crimes cometidos por meio da inteligência artificial, especialmente diante do surgimento de condutas inovadoras que ainda não encontram tipificação adequada no

ordenamento jurídico. Entre os crimes facilitados ou potencializados por IA, destacam-se a criação e disseminação de deepfakes para fins de extorsão, manipulação de eleições por meio de bots automatizados, ataques de phishing hiperpersonalizados, fraudes financeiras com uso de algoritmos de aprendizado de máquina e a automação de ataques de ransomware. Tais práticas afetam diretamente a população, seja por meio da erosão da confiança em informações públicas, prejuízos financeiros, exposição de dados sensíveis ou danos à reputação de indivíduos e empresas. A dificuldade em tipificar e punir esses crimes decorre, em grande parte, da velocidade com que as tecnologias evoluem, superando a capacidade do legislador de prever e descrever condutas ilícitas de modo preciso. Além disso, a natureza transnacional dos crimes digitais, a complexidade técnica das infraestruturas envolvidas e a ausência de consenso internacional sobre definições e fronteiras desses delitos tornam ainda mais árduo o processo legislativo e a efetiva responsabilização dos agentes, perpetuando um cenário de insegurança jurídica e vulnerabilidade social, como apoia o autor Rocha (2022).

Segundo estudos publicados na Enciclopédia Jurídica da PUCSP (2024), a rápida evolução tecnológica, em especial com o advento da inteligência artificial (IA), expôs de maneira contundente a insuficiência das normas jurídicas atualmente vigentes no Brasil. Embora o país tenha avançado com o Marco Civil da Internet e a Lei Geral de Proteção de Dados (LGPD), essas legislações não contemplam de forma específica e abrangente as novas dinâmicas trazidas por sistemas autônomos e algoritmos inteligentes. A ausência de marcos regulatórios claros para IA dificulta a responsabilização por danos causados por decisões automatizadas, além de não prever mecanismos de transparência e explicabilidade, essenciais para proteger direitos fundamentais dos cidadãos no ambiente digital.

Além disso, ainda de acordo com Rocha (2022), a legislação penal brasileira ainda se mostra anacrônica diante das sofisticadas práticas criminosas viabilizadas por novas tecnologias. O Código Penal, concebido em uma era pré-digital, não abarca condutas típicas de crimes cibernéticos complexos, como manipulação algorítmica, deepfakes, ataques automatizados e fraudes baseadas em IA. Essa lacuna normativa resulta em frequentes situações de atipicidade, nas quais condutas lesivas não encontram tipificação adequada, favorecendo a impunidade e estimulando a criatividade de agentes mal-intencionados.

Outro ponto crítico é a ausência de regulamentação sobre a coleta, processamento e uso de dados por sistemas de inteligência artificial, especialmente no que tange à proteção contra discriminação algorítmica e violações de privacidade. A LGPD, embora avance na proteção de dados pessoais, não impõe obrigações específicas para desenvolvedores e

operadores de IA quanto à mitigação de vieses, auditoria de decisões automatizadas e prestação de contas. Isso deixa os cidadãos vulneráveis a decisões opacas e potencialmente discriminatórias, sem mecanismos claros de contestação ou reparação. Sustentam Araujo, Silva e Azevedo (2024), através de seu artigo, ondem apoiam também a importância de desenvolver e aplicar a inteligência artificial em um contexto que respeite e promova os direitos humanos.

A falta de atualização legislativa também compromete a cooperação internacional no combate aos crimes digitais, como apoiam Oliveira e Carneiro Maia (2024), em seu trabalho ondem argumentam que um dos maiores desafios do campo jurídico é a imputação de culpabilidade quando os crimes são cometidos através da inteligência artificial. Neste quesito, sabe-se que o Brasil ainda não aderiu plenamente à Convenção de Budapeste, principal tratado internacional sobre cibercrime, o que dificulta a harmonização de procedimentos investigativos e a troca de informações com outros países. Em um cenário no qual cibercrimes frequentemente ultrapassam fronteiras, a inexistência de normas compatíveis com padrões internacionais limita a eficácia das investigações e a responsabilização de infratores.

Por fim, como expressa Peck (2021), a ausência de regulamentação específica para novas tecnologias gera comprovada insegurança jurídica tanto para usuários quanto para empresas inovadoras. A incerteza quanto à legalidade de determinadas práticas, à responsabilidade civil e penal por danos causados por sistemas autônomos, e à proteção de direitos individuais, pode inibir investimentos e o desenvolvimento tecnológico nacional. Assim, torna-se urgente a elaboração de um marco legal específico para inteligência artificial e outras tecnologias emergentes, visando garantir a segurança jurídica, a proteção dos direitos fundamentais e a promoção da inovação responsável.

Além disto, como apoiam as ideias de Teixeira (2025), é inevitável a necessidade da criação de um órgão específico para o monitoramento e persecução de cibercrimes, principalmente aqueles cometidos através da Ias; possibilitando ao braço da lei acompanhar e alcançar os infratores na mesma velocidade com que as tecnologias evoluem, garantindo que crimes digitais não fiquem impunes por ausência de tipificação ou meios eficazes de punição, além de assegurar a prevenção e o combate efetivo a essas infrações por meio de informações adequadas e atuação específica.

2.2.7 A Convenção de Budapeste e os Desafios da Tipificação dos Cibercrimes no Brasil

A Convenção de Budapeste (2001), promulgada pelo Brasil em 2023, foi um marco internacional ao estabelecer que apenas condutas dolosas devem ser consideradas cibercrimes. Essa diretriz evita que usuários

comuns, sem conhecimento técnico, sejam responsabilizados por ações involuntárias, como o reenvio acidental de vírus. No Brasil, essa orientação é para que a legislação penal não criminalize condutas culposas e para garantir que apenas quem age com intenção de causar dano seja punido. A Convenção também enfatiza a necessidade de precisão terminológica na tipificação dos crimes, protegendo bens jurídicos como confidencialidade, integridade e disponibilidade dos sistemas e dados informáticos.

Apesar dos avanços em normas como o Marco Civil da Internet e a Lei Geral de Proteção de Dados, o Brasil ainda possui poucas leis específicas para combater a criminalidade virtual. O princípio da anterioridade penal, previsto no artigo 1º do Código Penal, determina que só pode ser punido o que estiver tipificado em lei. Assim, a escassez de tipos penais para crimes cibernéticos pode transformar o Brasil em um ambiente propício para cibercriminosos, pois muitas condutas lesivas não encontram respaldo legal para serem punidas, apoia Barreto e Brasil (2016).

A criação da Convenção de Budapeste, do ano de 2001, com mais de sessenta países signatários, buscou uniformizar e fortalecer o combate ao cibercrime, promovendo a cooperação internacional e a adoção de legislações adequadas. O documento aborda desde definições e tipificações penais até medidas processuais e cooperação entre Estados, reconhecendo a necessidade de parcerias entre setor público e privado. O caráter transnacional dos cibercrimes exige essa abordagem coordenada para evitar conflitos de jurisdição e garantir a efetividade das investigações.

> […] tipifica os principais crimes cometidos na internet e prioriza, conforme o seu preâmbulo, uma política criminal comum, com o objetivo de proteger a sociedade contra a criminalidade no ciberespaço, pela adoção de legislação adequada e pela melhoria da cooperação internacional neste campo; reconhecendo, portanto, a necessidade de uma cooperação entre os Estados e com a participação da iniciativa privada (Teixeira, 2024; p. 623 á 637).

A Convenção é dividida em capítulos que tratam de terminologias, tipificação penal, cooperação internacional e disposições finais. No âmbito penal, tipifica crimes contra sistemas e dados informáticos, pornografia infantil e violações de direitos autorais, sempre exigindo a presença do dolo. No campo processual, prevê medidas como preservação e busca de dados, coleta em tempo real e regras para cooperação internacional, adaptando procedimentos clássicos à realidade digital e à volatilidade das provas eletrônicas.

No Brasil a Lei 12.737/2012, conhecida como Lei Carolina Dieckmann, segundo Teixeira (2024), foi inspirada, em parte, na Convenção de Budapeste, inseriu o artigo 154-A no Código Penal para tipificar a invasão de dispositivos informáticos. No entanto, a lei foi considerada limitada, não abrangendo todas as modalidades de cibercrime nem

acompanhando as diretrizes internacionais. Questiona também se a lei foi capaz de, efetivamente, combater os crimes cibernéticos e se as medidas de criminalização foram proporcionais à gravidade das infrações.

Apesar de ter avançado na tipificação de alguns crimes digitais, a legislação brasileira ainda carece de maior precisão e abrangência para enfrentar os desafios do cibercrime. A ausência de normas específicas para práticas como engenharia reversa de software e a limitação na cooperação internacional mostram que há um longo caminho a ser percorrido.

> […] justamente porque não respeita fronteiras, a internet é muito mais ágil na disseminação de ameaças e no desrespeito às leis nacionais do que os governos em suas tentativas de ampliar aos crimes praticados pela internet as mesmas leis impostas aos cidadãos no mundo real; e que se entende como crime cibernético desde a distribuição de e-mails não desejados e criação de vírus até a promoção do tráfico de pessoas, crime organizado, corrupção, pedofilia, racismo etc (Teixeira, 2024; p. 623 à 637).

O fortalecimento da legislação e a integração com iniciativas internacionais, como as previstas pela União Europeia e pela Convenção de Budapeste, são de fato, bases para garantir a segurança jurídica, a proteção dos usuários e a efetividade no combate aos crimes cibernéticos no Brasil, como afirma o trabalho de Barreto, Kufa e Silva (2020).

2.2.8 Da Tipificação no Direito Digital e Do Papel do Advogado

No cenário atual, as transformações tecnológicas redefinem não apenas as estruturas sociais, mas também as bases do poder e da organização social. A informação tornou-se o principal recurso estratégico, influenciando diretamente as relações entre indivíduos e Estados, que agora são avaliados pela sua capacidade de acessar e manejar dados. Nesse contexto de constante evolução, o Direito Digital emerge como um campo que precisa acompanhar a fluidez das mudanças, adotando uma postura flexível e orientada por práticas jurídicas adaptativas e inovadoras.

Nas palavras de Patricia Peck :

> Na Era Digital, o instrumento de poder é a informação, não só recebida mas refletida. A liberdade individual e a soberania do Estado são hoje medidas pela capacidade de acesso à informação. Em vez de empresas, temos organizações moleculares, baseadas no Indivíduo. A mudança é constante e os avanços tecnológicos afetam diretamente as relações sociais. Sendo assim, o Direito Digital é, necessariamente, pragmático e costumeiro16, baseado em estratégia jurídica e dinamismo (Peck, 2021; p. 46).

Com o aumento da complexidade social impulsionada pela digitalização, o papel do advogado também se transforma, exigindo uma visão que ultrapassa o domínio exclusivo das normas jurídicas. Para atuar eficazmente, é importante que o profissional compreenda os diversos fatores que moldam as interações contemporâneas, incluindo aspectos econômicos,

tecnológicos e políticos, que influenciam diretamente as relações entre indivíduos, organizações e Estados. Essa abordagem estratégica é importante para navegar no ambiente jurídico multifacetado do mundo digital.

Peck (2021) afirma também, que, na sociedade digital, o advogado precisa atuar como um estrategista, pois a complexidade social implica uma maior complexidade jurídica. Segundo ele, não basta apenas conhecer o Direito e as leis; é necessário compreender também os modelos que orientam as relações entre pessoas, empresas, mercados e Estados.

Diante desse cenário, o advogado moderno precisa desenvolver habilidades analíticas e estratégicas que vão além da interpretação legal tradicional. É importante que ele compreenda as dinâmicas do mercado, as inovações tecnológicas e as transformações sociais que impactam as relações jurídicas. Somente assim será possível oferecer soluções eficazes e adaptadas às demandas de um mundo em constante mudança, onde o Direito deve ser um instrumento ágil e eficiente para a resolução de conflitos.

Para que essa atuação proativa e multidisciplinar seja efetiva, é vital que o ordenamento jurídico acompanhe as transformações tecnológicas e sociais, suprindo as lacunas existentes na legislação penal. Sem uma normatização específica e atualizada, torna-se difícil assegurar a responsabilização adequada dos agentes envolvidos nos crimes digitais, comprometendo a segurança jurídica e a proteção dos direitos na esfera virtual. Assim, a evolução das leis é peça-chave para que os profissionais do Direito possam exercer plenamente seu papel na construção de uma sociedade digital mais segura e justa.

A crescente complexidade dos delitos digitais deixa clara a insuficiência das normas penais tradicionais para abarcar todas as nuances dos crimes praticados no ambiente virtual. Essa lacuna normativa gera uma expectativa significativa por parte da comunidade jurídica e da sociedade em geral por uma legislação mais específica e atualizada, capaz de responder às demandas do mundo digital e garantir a efetiva responsabilização dos infratores.

> Há uma enorme expectativa e ansiedade para uma adequada normatização que trate da informática, especialmente no campo criminal, pois diante da ausência de legislação específica têm-se aplicado o Código Penal (que recentemente foi alterado para abrigar alguns poucos crimes relacionados à informática) e leis especiais.[...] Porém, outros delitos eventualmente podem não se enquadrar nos tipos penais estabelecidos até então, surgindo a denominada atipicidade do ato, com a consequente impunidade do agente criminoso (Teixeira, 2024; p. 623 a 637).

Essa lacuna legislativa, aliada à rápida evolução tecnológica, evidencia a urgência de um marco regulatório que não apenas preencha as atuais insuficiências, mas também antecipe os desafios futuros, como a responsabilização em sistemas automatizados. Com o avanço da inteligência artificial, torna-se imprescindível definir claramente quem deve responder pelas

decisões tomadas por agentes autônomos ou seus supervisores humanos, garantindo assim segurança jurídica e a possibilidade de estabelecer limites contratuais e mecanismos de proteção eficazes.

Além das dificuldades legislativas, a evolução tecnológica traz novos desafios para a regulação jurídica, especialmente com o avanço da inteligência artificial. A atribuição de responsabilidade em processos automatizados torna-se um tema central, exigindo que as normas prevejam claramente quem responde pelas decisões tomadas por sistemas de IA, seja o próprio agente artificial ou o supervisor humano. Essa delimitação garante a segurança jurídica e permite que os operadores do direito possam estabelecer limites contratuais e mecanismos de proteção adequados

> Pensando que vamos para um cenário com maior uso de Inteligência Artificial, as regulamentações têm também previsto que deve haver sempre alguém responsável pela tomada de decisão automatizada, ou seja, o agente de IA, ou o supervisor humano a quem caberá a responsabilidade. Se ela está sendo ampliada pelas leis, caberá aos juristas limitá-la nos pactos entre partes, através de cláusulas nos contratos e na aplicação de seguros (Peck, 2021; p. 308).

À medida que a inteligência artificial se torna cada vez mais presente em decisões automatizadas, é preciso que haja uma definição clara para garantir segurança jurídica e proteção aos envolvidos. No Brasil, essa necessidade tem impulsionado o desenvolvimento de um marco regulatório específico, como o Projeto de Lei n. 2.338/2023, que estabelece critérios para a responsabilização civil dos operadores e fornecedores de sistemas de IA, diferenciando regimes conforme o grau de risco do sistema. Essa regulamentação busca equilibrar a inovação tecnológica com a proteção dos direitos, adotando, por exemplo, a responsabilidade objetiva para sistemas de alto risco e mecanismos que facilitem a reparação de danos causados por falhas ou decisões automatizadas.

Essa necessidade de adaptação normativa reflete uma transformação mais ampla na sociedade, em que o Direito deve acompanhar as mudanças profundas nos modelos econômicos e sociais. A revolução digital redefine o conceito de valor e propriedade, exigindo que condutas antes consideradas triviais, como a criação de vírus ou o furto de dados por simples cópia, sejam efetivamente reconhecidas como ilícitos, com regras claras para sua prevenção e punição.

> Quando a sociedade muda, o Direito também deve mudar, evoluir. Estamos vivendo amterceira grande revolução da humanidade, em que há uma completa transformação no modelo de riqueza, agora baseado nos ativos intangíveis, e nos valores e regras estabelecidas para reger as relações socioeconômicas, onde fazer um vírus ou mesmo praticar um furto de dados com uso do recurso de “CTRL C CTRL V” tornam-se condutas que precisam ser tratadas (Peck, 2021; p. 336).

No contexto da rápida transformação digital e da crescente interconectividade global,

Peck (2021) destaca que os profissionais do Direito precisam superar divisões tradicionais e acadêmicas para desenvolver uma visão integrada e colaborativa. Essa nova realidade exige uma postura que valorize a convergência de ideias e a busca conjunta por soluções jurídicas capazes de responder às complexidades de uma sociedade em constante evolução tecnológica e social. Segundo o autor, a sociedade digital demanda que os operadores do Direito deixem de lado rivalidades acadêmicas para discutir conjuntamente paradigmas como ordenamento, legitimidade e segurança, sendo essa a postura que o mercado espera e que os profissionais devem adotar para atuar eficazmente nesse novo cenário.

Diante desse cenário de transformação acelerada, com base no trabalho de Teixeira (2024), a tipificação dos cibercrimes no ordenamento jurídico brasileiro representa um passo importante para o enfrentamento das novas formas de criminalidade digital. A inclusão de condutas específicas relacionadas à informática no Código Penal e em legislações especiais, demonstra o esforço do legislador em adaptar a legislação às demandas do ambiente virtual. Apesar desses avanços, ainda persistem lacunas importantes, especialmente diante da sofisticação dos delitos cibernéticos e do surgimento de novas tecnologias, como a inteligência artificial, que desafiam os limites das normas tradicionais e exigem constante atualização normativa.

Portanto, para garantir a efetiva proteção dos direitos e a responsabilização adequada dos agentes, é imprescindível que o ordenamento jurídico brasileiro continue evoluindo, promovendo a tipificação clara e abrangente dos cibercrimes. A atuação integrada entre Poder Público, operadores do Direito e sociedade civil é importante para o desenvolvimento de mecanismos de prevenção, investigação e punição eficazes. Somente assim será possível construir um ambiente digital mais seguro, capaz de acompanhar as transformações tecnológicas e assegurar a justiça diante dos desafios impostos pela era da informação.

3 CONSIDERAÇÕES FINAIS

A transformação digital trouxe inúmeros benefícios para a sociedade, mas também impôs desafios inéditos ao Direito, especialmente no que se refere à segurança e proteção dos cidadãos no ambiente virtual. O aumento dos crimes cibernéticos no Brasil exige respostas rápidas e eficazes do legislador e dos operadores do Direito, diante da crescente complexidade das relações sociais e dos delitos digitais que acompanham a evolução tecnológica.

A cibercultura, ao integrar as tecnologias digitais no cotidiano, ampliou as possibilidades de atuação criminosa, criando um ambiente propício para novos tipos de crimes

devido à facilidade de acesso à informação, ausência de barreiras físicas e anonimato na internet. Embora o ordenamento jurídico brasileiro tenha avançado, ainda existem lacunas que dificultam a responsabilização e prevenção eficaz dos crimes digitais, especialmente diante do uso de tecnologias sofisticadas.

A tipificação dos cibercrimes no Brasil está em constante construção e deve acompanhar as rápidas transformações tecnológicas e sociais para garantir a proteção dos direitos, responsabilizar os infratores e promover um ambiente digital mais seguro e justo.

Durante a realização desta pesquisa, uma limitação significativa foi a dificuldade de encontrar estatísticas atualizadas sobre a incidência de cibercrimes, a efetividade das investigações e o perfil das vítimas e dos criminosos. A ausência desses dados quantitativos compromete uma análise mais aprofundada do fenômeno e limita a fundamentação de propostas de políticas públicas mais assertivas.

A tipificação dos cibercrimes no Brasil está em constante construção e deve acompanhar as rápidas transformações tecnológicas e sociais para garantir a proteção dos direitos, responsabilizar os infratores e promover um ambiente digital mais seguro e justo.

Em síntese, tal problemática demanda um esforço contínuo e integrado, pois somente por meio dessa articulação será possível construir um ambiente digital onde os direitos dos cidadãos sejam efetivamente protegidos e os agentes criminosos responsabilizados. Para que essa evolução seja efetiva, é interessante adotar uma abordagem que combine avanços tecnológicos e ações jurídicas., investir no desenvolvimento de tecnologias de segurança sofisticadas, como a inteligência artificial, aprimora a capacidade de detectar e neutralizar ameaças cibernéticas com maior precisão e agilidade.

Além disso, a criação de uma entidade dedicada ao monitoramento constante das ameaças virtuais é imprescindível, promovendo a cooperação entre diferentes órgãos e o compartilhamento de recursos, fortalecendo assim a proteção dos direitos dos cidadãos e assegurando a responsabilização dos infratores no ambiente digital.

No tocante às perspectivas para pesquisas futuras, destaca-se a importância de realizar análises comparadas com experiências internacionais, a fim de identificar boas práticas e estratégias eficazes adotadas por outros países no enfrentamento aos crimes cibernéticos. Recomenda-se, ainda, a criação e avaliação de órgãos especializados em segurança cibernética, tanto em âmbito nacional quanto em articulação com iniciativas globais, para aprimorar a prevenção, investigação e repressão desses delitos.

Dessa forma, o Direito pode se manter em constante evolução, acompanhando as transformações da era digital e promovendo soluções jurídicas que respondam às

complexidades do mundo contemporâneo.

REFERENCIAS

Araújo, A. da S., Silva, C. de S. da, & Azevedo, D. do C. (2024). Criminalização Do Uso Indevido Da Inteligência Artificial: Desafios Legais E Impactos Na Responsabilidade Penal. **Revista Ibero-Americana De Humanidades, Ciências E Educação**, 10(12), p.147–162. https://doi.org/10.51891/rease.v10i12.17230. Acesso em 22 de Maio de 2025.

BARRETO, Alessandro Gonçalves; BRASIL, Beatriz Silvera. **Manual de Investigação Cibernética:** à Luz do Marco Civil da Internet. Rio de Janeiro: Editora Brasport, 2016.

BARRETO, Alessandro Gonçalves; KUFA, Karina; SILVA, Marcelo Mesquita. **Cibercrimes e Seus Reflexos no Direito Brasileiro**. Salvador: Editora Juspodivm, 2020, p, 123-138.

Belli; Nougrères, et al. **Transferência internacional de dados pessoais na América Latina:** rumo à harmonização de normas. Rio de Janeiro: Lumen Juris, 2024. Disponível em: https://ppl-ai-file-upload.s3.amazonaws.com/web/direct-files/attachments/29580268/5b5497fb-77bc-48ba-9f6c-742fa7c64570/transferencia-internacional-de-dados-pessoais-na-america-latina_ebook-1.pdf. Acesso em 20 de Maio de 2025.

BORGES, Fabiani. **Terrorismo Cibernético e a Proteção de Dados Pessoais.** 2015, p. 1. Disponível em: https://fabianiborges.jusbrasil.com.br/artigos/218335957/terrorismo-cibernetico-e-a-protecaode-dados-pessoais.Acesso em 12 de Maio de 2025.

BRASIL. Ministério Público Federal. **Convenção Sobre o Cibercrime**. Budapeste, 23 nov. 2001. Disponível em: http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf. Acesso em 22 de Abril de 2025.

BRASIL. Ministério Público Federal. **Minuta do Relatório Explicativo**. Disponível em:http://www.mpf.mp.br/atuacao-tematica/ccr2/coordenacao/comissoes-e-grupos-de-trabalho/combate-crimes-cirberneticos/convention-on-cybercrime/explanatory-reports_pt.pdf.Acesso em 12 de Março de 2025.

CARVALHO, Freedy. **Você na era digital**: os desafios da revolução da comunicação, 2014, p.1. Disponível em: http://www.mk2.com.br/mk2/voce-na-era-digital-os-desafios-da-revolucao-na-comunicacao.asp. Acesso em 22 de Maio de 2025.

COSTA, Ana Maria Nicolaci da. **Na malha da rede**: Os impactos íntimos da internet. Rio de Janeiro: Campus, 1998, p.17.

DESLANDES, Maria S.S.; ARANTES, Álisson R.. **Os perigos dos crimes virtuais nas redes sociais.** 2017, p.175. Disponível em: https://periodicos.pucminas.br/index.php/sinapsemultipla/article/view/16488/12745.Acesso em 10 de Março de 2025.

EUROPOL. **Steal, deal and repeat**: How cybercriminals trade and exploit your data Internet Organised Crime Threat Assessment (IOCTA) 2025. https://www.europol.europa.eu/publication-events/main-reports/steal-deal-and-repeat-

how-cybercriminals-trade-and-exploit-your-data#downloads. Acesso em 17 de Março de 2025.

FIORILLO, Celso Antonio Pacheco. **Princípios constitucionais do direito da sociedade da informação.** São Paulo: Saraiva, 2014, p. 18-19.Acesso em 20 de Fevereiro de 2025.

Fundação Getulio Vargas (FGV). (2023). **Transferência internacional de dados pessoais na América Latina**. Rio de Janeiro: FGV Direitorio. Disponível em: https://direitorio.fgv.br/sites/default/files/arquivos/transferencia-internacional-de-dados-pessoais-na-america-latina_ebook.pdf.Acesso em 22 de Fevereiro de 2025.

Guidi, G. B. C., & Rezek, F. (2023). **Crimes na internet e cooperação internacional em matéria penal entre Brasil e Estados Unidos**. Revista Brasileira de Política Pública, 8(1). DOI: 10.5102/rbpp.v8i1.5130. Disponível em: https://www.publicacoesacademicas.uniceub.br/RBPP/article/download/5130/3713.Acesso em 17 de Março de 2025.

IBDFAM – Instituto Brasileiro do Direito de Familia. **Brasil adere à Convenção sobre o Crime Cibernético**. 2023. https://ibdfam.org.br/noticias/10707/Brasil+adere+%C3%A0+Conven%C3%A7%C3%A3o+sobre+o+Crime+Cibern%C3%A9tico. Acesso em 19 de Março de 2025.

IBGE - Instituto Brasileiro de Geografia e Estatística. **Pesquisa Pulso Empresa**: Impacto da Covid-19 nas empresas, 2020, P.1, https://www.ibge.gov.br/estatisticas/sociais/saude/28291-pesquisa-pulso-empresa-impacto-da-covid-19-nas-empresas.html.Acesso em 25 de Março de 2025.

INTERPOL. (2020). **Cybercrime**: COVID-19 Impact. Disponível em: https://www.interpol.int/en/News-and-Events/News/2020/Cybercrime-COVID-19-impact.Acesso em 12 de Maio de 2025.

IPEA – Instituto de Pesquisa Econômica Aplicada. **Estudo evidencia o impacto devastador da pandemia para micro e pequenas empresas**, 2023, p.1, https://www.ipea.gov.br/portal/categorias/45-todas-as-noticias/noticias/13845-estudo-evidencia-o-impacto-devastador-da-pandemia-para-micro-e-pequenas-empresas.Acesso em 21 de Maio de 2025.

LEMOS, André. **Palestra: Cibercultura**. 2003, p.1. Disponível em: http://www.facom.ufba.br/ciberpesquisa.Acesso em 12 de Abril de 2025.

LNCC - Laboratório Nacional de Computação Científica. **Ponto memória: ciência e independência**, 2022, p.1 https://www.gov.br/lncc/pt-br/assuntos/noticias/ultimas- noticias-1/ponto-de-memoria-ciencia-e-independencia.Acesso em 12 de Maio de 2025.

MJSP - Ministério da Justiça e Segurança Pública. **PF cumpre mandado de busca e apreensão para reprimir o armazenamento de imagens de abuso sexual infantojuvenil**.2025.https://www.gov.br/pf/pt-br/assuntos/noticias/2025/02/pf-cumpre-mandado-de-busca-e-apreensao-para-reprimir-o- armazenamento-de-imagens-de-abuso-sexual-infantojuvenil.Acesso em 23 de Maio de 2025.

MJSP - Ministério da Justiça e Segurança Pública. **PF deflagra operações contra fraudes cibernéticas, lavagem de dinheiro e tráfico de drogas.** 2025.https://www.gov.br/pf/pt-br/assuntos/noticias/2025/05/pf-deflagra-operacoes-contra-fraudes-ciberneticas-lavagem-de-dinheiro-e-trafico-de-drogas.Acesso em 23 de Maio de 2025.

PESQUISA FAPESP, **Revista Primordios da Rede** - A história dos primeiros momentos da internet no Brasil. 2011, p.1, https://revistapesquisa.fapesp.br/prim%C3%B3rdios-da-rede_/.Acesso em 22 de Maio de 2025.

PINHEIRO, Patrícia Peck. **Direito Digital**. 8. ed. São Paulo: Saraiva, 2021, p.41;49-338.

PLANALTO. **Convenção sobre o Crime Cibernético**. DECRETO Nº 11.491, DE 12 DE ABRIL DE 2023.https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11491.htm. Acesso em 06 de Março de 2025.

PLANALTO. **Convenção de Budapeste, decreto nº 11.491, de 12 de Abril de 2023.** https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11491.htm.Acesso em 06 de Março de 2025.

PLANALTO. **Lei Carolina Dickman, Nº 12.737, de 30 de Novembro de 2012.** https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm.Acesso em 07 de Março de 2025.

PLANALTO. **Projeto de Lei nº 2.338/2023,** https://www25.senado.leg.br/web/atividade/materias/-/materia/157233.Acesso em 07 de Abril de 2025.

RAZZOUK, D. **Dependência de Internet**: uma nova categoria diagnostica?. 1998, p.1. Disponível em http://wwwpriory.com/psych/dpnet.htmm.Acesso em 05 de Março de 2025.

Rocha, J. H. L. (2022). Revista FT. **Crimes cibernéticos e inteligência artificial.** 2022. https://revistaft.com.br/crimes-ciberneticos-e-inteligencia-artificial/.Acesso em 19 de Abril de 2025.

ROSSINI, Augusto Eduardo de Souza. **Informática, telemática e direito penal**. São Paulo: Memória Jurídica, 2004, p.110.

SIQUEIRA, Marcela Scheuer et al. **Crimes virtuais e a legislação brasileira**. (Re)Pensando o Direito – Rev. do Curso de Graduação em Direito da Faculdade CNEC Santo Ângelo. v. 7, n. 13 (2017).

SILVA, Rita de Cássia Lopes. **Direito penal e sistema informático**. São Paulo: Revista dos Tribunais, 2003, p.28.

TEIXEIRA, Tarcisio. **Direito Digital e Processo Eletronico.** 2024, p.623-637.

Verbete PUC-SP. **IA e a lei brasileira de responsabilidade e transparência na internet**. Tomo Direito Econômico, Edição 1, Março de 2024. https://enciclopediajuridica.pucsp.br/verbete/577/edicao-1/a-inteligencia-artificial-%28ia%29-e-a-lei-brasileira-de-responsabilidade-e-transparencia-na-internet---humanismo-4.0---impactos-na-cidadania. Acesso em 22 de Maio de 2025.