UNIVERSIDADE PAULISTA – UNIP

VICTÓRIA HELENA FERNANDES DE OLIVEIRA

NOTA 10

O DIREITO DIGITAL NO BRASIL:

UMA ANÁLISE DO SISTEMA JURÍDICO BRASILEIRO NO ENFRENTAMENTO AOS CRIMES DIGITAIS

SANTOS

2026

VICTÓRIA HELENA FERNANDES DE OLIVEIRA

O DIREITO DIGITAL NO BRASIL:

UMA ANÁLISE DO SISTEMA JURÍDICO BRASILEIRO NO ENFRENTAMENTO AOS CRIMES DIGITAIS

Trabalho de Conclusão de Curso para obtenção do título de graduação em Bacharelado em Direito apresentado à Universidade Paulista – UNIP.

Orientador: Prof. Dr. Raphael Feitosa Fissore.

SANTOS

2026

CIP - Catalogação na Publicação

Oliveira, Victória Helena Fernandes.
O DIREITO DIGITAL NO BRASIL: UMA ANÁLISE DO SISTEMA JURÍDICO BRASILEIRO NO ENFRENTAMENTO AOS CRIMES DIGITAIS / Victória Helena Fernandes Oliveira. – 2026.
47 f.

Trabalho de Conclusão de Curso (Graduação) apresentado ao Instituto de Ciência Jurídicas da Universidade Paulista, Santos, 2026.
Área de Concentração: Direito Digital.
Orientador: Prof. Dr. Raphael Feitosa Fissore.

1. Direito Digital. 2. Direito Penal. 3. Crimes Digitais. 4. Inteligência Artificial . 5. Proteção de Dados. I. Fissore, Raphael Feitosa (orientador). II. Título.

Elaborada pelo Sistema de Geração Automática de Ficha Catalográfica da Universidade Paulista com os dados fornecidos pelo(a) autor(a).

VICTÓRIA HELENA FERNANDES DE OLIVEIRA

O DIREITO DIGITAL NO BRASIL:

UMA ANÁLISE DO SISTEMA JURÍDICO BRASILEIRO NO ENFRENTAMENTO AOS CRIMES DIGITAIS

Trabalho de Conclusão de Curso para obtenção do título de graduação em Bacharelado em Direito apresentado à Universidade Paulista – UNIP.

Aprovado em:

BANCA EXAMINADORA

_____/_/_____

Prof. Dr. Raphael Feitosa Fissore

Universidade Paulista – UNIP

_____/_/_____

Universidade Paulista – UNIP

AGRADECIMENTOS

Agradeço, primeiramente, a Deus, por ter me sustentado ao longo de todos os meus dias, permitindo-me vivenciar Suas bênçãos e me concedendo força e sabedoria para chegar até aqui.

À minha mãe, por todo amor, incentivo e apoio incondicional em cada uma das minhas decisões, sendo minha maior fonte de inspiração. Ao meu pai e à minha avó, por todo o suporte e por contribuírem de forma essencial para a realização deste sonho. À minha irmã, por sempre estar ao meu lado, especialmente nos momentos mais difíceis, trazendo leveza e me ajudando a enfrentar os períodos de maior tensão.

Aos professores da Universidade Paulista – UNIP, que foram fundamentais na minha trajetória acadêmica, contribuindo significativamente para minha formação. Em especial, aos meus orientadores, Anderson Real e Raphael Fissore, pela paciência, dedicação e carisma, tornando possível a construção deste trabalho com alegria e satisfação.

Por fim, agradeço a todos que, de alguma forma, cruzaram meu caminho ao longo desses cinco anos e contribuíram para a minha formação pessoal e acadêmica. Cada experiência vivida foi essencial para que eu me tornasse quem sou hoje, e por isso sou profundamente grata.

RESUMO

O presente trabalho tem como objetivo analisar a atuação do sistema jurídico brasileiro no enfrentamento aos crimes digitais, considerando os instrumentos normativos existentes e a interpretação conferida pelo Poder Judiciário. A crescente utilização das tecnologias da informação e da comunicação tem ampliado a incidência de práticas ilícitas no ambiente virtual, exigindo do Direito constante adaptação às novas dinâmicas sociais e tecnológicas. Nesse contexto, a pesquisa examinou os fundamentos conceituais do Direito Digital, a classificação dos crimes digitais e as principais normas aplicáveis no ordenamento jurídico brasileiro, com destaque para o Marco Civil da Internet, a Lei Geral de Proteção de Dados e a Lei Carolina Dieckmann. A metodologia adotada consiste em revisão de literatura e documental, com análise de doutrina, legislação e jurisprudência, especialmente dos tribunais superiores. Ao longo do estudo, identificaram-se avanços relevantes na construção de um arcabouço normativo voltado à regulação do ambiente digital, bem como na atuação do Poder Judiciário na adaptação de institutos jurídicos tradicionais às novas realidades tecnológicas. Entretanto, também foram evidenciadas limitações estruturais, lacunas legislativas e desafios relacionados à investigação e à responsabilização de condutas ilícitas, especialmente diante da transnacionalidade dos crimes digitais e do avanço de tecnologias como a inteligência artificial. Conclui-se que, embora o sistema jurídico brasileiro tenha evoluído significativamente no enfrentamento da criminalidade digital, ainda se faz necessário o contínuo aprimoramento das normas, das instituições e dos mecanismos de cooperação, a fim de garantir maior efetividade na proteção de direitos no ambiente digital.

Palavras-chave: Direito Digital. Crimes digitais. Sistema jurídico brasileiro. Internet. Proteção de dados.

ABSTRACT

This study aims to analyze the role of the Brazilian legal system in addressing cybercrimes, considering both existing legal instruments and the interpretation provided by the Judiciary. The increasing use of information and communication technologies has expanded the occurrence of illicit practices in the digital environment, requiring constant adaptation of the law to new social and technological dynamics. In this context, the research examined the conceptual foundations of Digital Law, the classification of cybercrimes, and the main legal frameworks applicable in Brazil, with emphasis on the Civil Rights Framework for the Internet, the General Data Protection Law, and the Carolina Dieckmann Law. The methodology adopted consists of bibliographic and documentary research, based on the analysis of doctrine, legislation, and case law, especially from higher courts. Throughout the study, relevant advances were identified in the construction of a normative framework aimed at regulating the digital environment, as well as in the Judiciary's role in adapting traditional legal concepts to new technological realities. However, structural limitations, legislative gaps, and challenges related to the investigation and accountability of illicit conduct are also highlighted, particularly in view of the transnational nature of cybercrimes and the advancement of technologies such as artificial intelligence. It is concluded that, although the Brazilian legal system has significantly evolved in combating cybercrime, continuous improvement of legal norms, institutions, and cooperation mechanisms is still necessary to ensure greater effectiveness in protecting rights in the digital environment.

Keywords: Digital Law. Cybercrimes. Brazilian legal system. Internet. Data protection.

SUMÁRIO

1 INTRODUÇÃO 9
2 DIREITO DIGITAL E CRIMES DIGITAIS: FUDAMENTOS CONCEITUAIS E CLASSIFICAÇÃO 11
2.1 Conceito e evolução do Direito Digital no Brasil 11
2.2 Conceito e terminologia dos crimes digitais 14
2.3 Classificação e principais modalidades de crimes digitais 14
2.4 Características estruturais dos crimes digitais e seus impactos jurídicos e sociais 16
3 O TRATAMENTO JURÍDICO DOS CRIMES DIGITAIS NO ORDENAMENTO BRASILEIRO 19
3.1 Marco Civil da Internet – Lei n° 12.965/2014 19
3.2 Lei Geral de Proteção de Dados – Lei n° 13.709/2018 20
3.3 Lei Carolina Dieckmann – Lei n° 12.737/2012 21
3.4 Outras normas relevantes no enfrentamento dos crimes digitais 22
4 UMA ANÁLISE DO SISTEMA JURÍDICO BRASILEIRO NO ENFRENTAMENTO AOS CRIMES DIGITAIS 25
4.1 Limitações estruturais e investigativas do sistema jurídico brasileiro 25
4.2 Lacunas legislativas e insegurança jurídica no enfrentamento dos crimes digitais 28
4.3 Inteligência artificial e novos desafios à responsabilização jurídica 30
4.4 Normas de segurança da informação e proteção de dados 32
4.5 Avanços normativos e institucionais no enfrentamento dos crimes digitais: a atuação do STJ e do STF 34
4.6 Síntese crítica do sistema jurídico brasileiro aos crimes digitais e perspectivas diante das transformações tecnológicas 37
5 CONCLUSÃO 40
REFERÊNCIAS 43
BIBLIOGRAFIA 46

1 INTRODUÇÃO

O avanço das tecnologias da informação e da comunicação nas últimas décadas transformou profundamente a forma como as pessoas se relacionam, trabalham e se comunicam. A internet passou a ocupar um papel central na vida cotidiana, permitindo maior circulação de informações, facilitação de atividades econômicas e ampliação das formas de interação social. Ao mesmo tempo, esse ambiente digital também passou a ser utilizado para a prática de condutas ilícitas, dando origem ao fenômeno conhecido como crimes digitais.

Com o aumento da utilização da internet e das ferramentas tecnológicas, diferentes modalidades de crimes passaram a ocorrer no ambiente virtual, como fraudes eletrônicas, invasões de dispositivos informáticos, divulgação indevida de dados pessoais e outras práticas que podem causar prejuízos relevantes a indivíduos e instituições. Nesse contexto, o Direito passou a enfrentar o desafio de acompanhar essas transformações, buscando criar mecanismos jurídicos capazes de regular as relações estabelecidas no meio digital e de responsabilizar condutas ilícitas praticadas nesse espaço.

No Brasil, algumas iniciativas legislativas foram desenvolvidas com o objetivo de disciplinar o uso da internet e enfrentar determinados comportamentos ilícitos no ambiente digital. Entre essas medidas, destacam-se o Marco Civil da Internet[1], que estabeleceu princípios e diretrizes para o uso da internet no país, a Lei Carolina Dieckmann[2], responsável por tipificar penalmente determinadas condutas relacionadas à invasão de dispositivos informáticos, e a Lei Geral de Proteção de Dados Pessoais[3], que trouxe importantes regras voltadas à proteção de dados pessoais e à privacidade dos usuários.

Apesar desses avanços, o enfrentamento dos crimes digitais ainda apresenta diversos desafios. A própria dinâmica da internet, marcada pela rapidez das

[1] BRASIL. Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 05 abril 2025
[2] BRASIL. Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 07 abril 2025;
[3] BRASIL. Lei nº 12.737, de 30 de novembro de 2012 (Lei Carolina Dieckmann). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 16 abril 2025

transformações tecnológicas e pela circulação global de informações, muitas vezes dificulta a investigação de determinadas práticas ilícitas e a responsabilização de seus autores. Além disso, o surgimento constante de novas tecnologias exige que o Direito esteja em permanente processo de adaptação, tanto do ponto de vista legislativo quanto interpretativo.

Diante desse cenário, o presente trabalho tem como objetivo analisar de que forma o sistema jurídico brasileiro tem buscado enfrentar os crimes digitais, considerando tanto os instrumentos normativos existentes quanto a atuação do Poder Judiciário na interpretação dessas normas. A pesquisa procura compreender quais são os principais mecanismos jurídicos utilizados nessa esfera e quais desafios ainda permanecem na tentativa de garantir maior segurança no ambiente digital.

A relevância do tema está relacionada ao crescimento constante das práticas ilícitas realizadas por meio da internet e aos impactos que essas condutas podem gerar para a sociedade. Questões envolvendo privacidade, proteção de dados, segurança da informação e responsabilidade no ambiente digital têm se tornado cada vez mais presentes no debate jurídico contemporâneo, o que reforça a importância de estudos voltados à compreensão dessas transformações.

Para o desenvolvimento deste trabalho, foi realizada pesquisa de natureza bibliográfica e documental, com análise de legislação, doutrina e decisões judiciais relacionadas ao tema. O estudo busca, assim, apresentar uma reflexão acerca do atual cenário do Direito Digital no Brasil, destacando avanços normativos, interpretações jurisprudenciais e os principais desafios enfrentados pelo ordenamento jurídico diante das transformações tecnológicas.

Por fim, o trabalho encontra-se estruturado de forma a apresentar inicialmente uma contextualização sobre os crimes digitais e o surgimento do Direito Digital como área jurídica em desenvolvimento. Em seguida, são analisados os principais instrumentos normativos relacionados ao tema, bem como a atuação do Poder Judiciário na interpretação dessas normas. Ao final, realiza-se uma síntese crítica acerca da atuação do sistema jurídico brasileiro no enfrentamento dos crimes digitais e das perspectivas diante das transformações tecnológicas.

2. DIREITO DIGITAL E CRIMES DIGITAIS: FUNDAMENTOS CONCEITUAIS E CLASSIFICAÇÃO JURÍDICAS

2.1 Conceito e evolução do Direito Digital no Brasil

O avanço acelerado das tecnologias da informação e da comunicação transformou profundamente as formas de interação social, econômica e institucional, exigindo do Direito uma adaptação contínua às novas dinâmicas estabelecidas no ambiente virtual. Nesse cenário, surge o Direito Digital não como um ramo jurídico isolado, mas como uma evolução do próprio Direito, que incorpora princípios, institutos e normas já consolidados, reinterpretando-os à luz da realidade tecnológica contemporânea.

Essa compreensão afasta a ideia de que o meio digital constitui uma esfera dissociada do mundo real. Ao contrário, as relações jurídicas estabelecidas no ambiente virtual produzem efeitos concretos e relevantes, demandando respostas normativas eficazes. Conforme sustenta Patrícia Peck Pinheiro, o Direito Digital representa a adaptação do ordenamento jurídico às mudanças comportamentais e às novas formas de controle de condutas decorrentes do uso intensivo da tecnologia, reafirmando a necessidade de integração entre o direito tradicional e a realidade digital.[4]

Sob uma perspectiva doutrinária clássica, o Direito Digital pode ser compreendido como o conjunto de normas e instituições jurídicas voltadas à regulação do uso dos sistemas computacionais, seja como meio, seja como finalidade, sempre que tais sistemas incidirem sobre bens jurídicos relevantes da sociedade. Nesse sentido, Mario Antônio Lobato de Paiva destaca que esse campo jurídico abrange tanto as relações decorrentes da criação e utilização de softwares quanto aquelas estabelecidas no comércio eletrônico e nas interações humanas mediadas pela internet.[5]

---

[4] PINHEIRO, Patrícia Peck. Direito Digital. 7. ed. São Paulo: Saraiva, 2021

[5] COELHO, Rafael Paulo. A sociedade digital. Jusbrasil. Disponível em: https://www.jusbrasil.com.br/artigos/direito-digital/1961307356 . Acesso em: 07 abr. 2025.

Em complemento, Almeida Filho conceitua o Direito Digital como o conjunto de normas e construções doutrinárias destinadas a regular toda relação jurídica em que a informática se apresenta como elemento central, gerando direitos e deveres correlatos.[6] Tal definição reforça o caráter transversal e interdisciplinar do Direito Digital, uma vez que dialoga com diversos ramos do Direito, como o Civil, o Penal, o Empresarial e o Constitucional.

Nesse âmbito, o Direito Digital envolve diversas questões relacionadas à preservação da privacidade, à segurança da informação e à proteção de dados pessoais, além de temas ligados à liberdade de manifestação no ambiente virtual. A transferência progressiva das interações sociais e econômicas para o espaço digital passou a exigir do sistema jurídico não apenas a releitura de normas tradicionais, mas também a criação de novos mecanismos normativos capazes de assegurar a efetiva proteção dos direitos fundamentais e a estabilidade das relações jurídicas.

É possível identificar, nesse cenário, dois principais eixos de atuação do Direito Digital. O primeiro é o legislativo, voltado à elaboração de normas específicas destinadas a disciplinar condutas praticadas no ambiente virtual e tipificar novos ilícitos decorrentes do uso da tecnologia. O segundo é o interpretativo, que consiste na aplicação das normas já existentes a situações que passaram a ocorrer no meio digital, considerando suas particularidades técnicas e sociais.

Destaca-se ainda o caráter transnacional do Direito Digital, uma vez que as tecnologias digitais transcendem fronteiras geográficas e possibilitam a circulação instantânea de informações em escala global. Tal característica impõe desafios adicionais aos sistemas jurídicos nacionais, exigindo cooperação internacional e a construção de parâmetros comuns de responsabilização e proteção de direitos no ambiente virtual.

A expansão da internet em escala mundial, especialmente a partir da década de 1990, marcou uma profunda transformação nas formas de comunicação, produção e circulação de informações, impactando diretamente as relações sociais, econômicas e jurídicas. A popularização do acesso à rede mundial de computadores evidenciou a

[6] COELHO, Rafael Paulo. A sociedade digital. Jusbrasil. Disponível em: https://www.jusbrasil.com.br/artigos/direito-digital/1961307356. Acesso em: 07 abr. 2025.

insuficiência do ordenamento jurídico tradicional para lidar com situações inéditas decorrentes do ambiente virtual.

No Brasil, os primeiros esforços institucionais voltados à organização e ao uso da internet ocorreram ainda em meados da década de 1990, com a criação do Comitê Gestor da Internet no Brasil, em maio de 1995, responsável por estabelecer diretrizes técnicas e fomentar o desenvolvimento da rede no país. Nesse mesmo período, a regulamentação do uso da internet ainda era incipiente e fragmentada. Um dos primeiros instrumentos normativos relacionados ao tema foi a Portaria Interministerial nº 147, de 31 de maio de 1995, que disciplinou a utilização da rede pública de telecomunicações para a prestação de serviços de conexão à internet.[7]

Com o crescimento acelerado do número de usuários da internet no Brasil, tornaram-se mais evidentes as fragilidades normativas relacionadas à proteção de direitos e à repressão de condutas ilícitas praticadas no ambiente virtual. Atualmente, o país figura entre as nações com maior número de usuários conectados, com mais de 139 milhões de pessoas com acesso regular à internet.[8] Ante essa situação, o Poder Judiciário passou a desempenhar papel relevante na adaptação do Direito às novas demandas tecnológicas, aplicando normas já existentes a conflitos surgidos no ambiente virtual por meio da analogia, dos costumes e dos princípios gerais do Direito.

A consolidação normativa do ambiente digital brasileiro ocorreu de forma mais estruturada nas décadas seguintes, especialmente com a promulgação do Marco Civil da Internet e, posteriormente, da Lei Geral de Proteção de Dados Pessoais. Paralelamente ao desenvolvimento dessa estrutura normativa, a expansão das tecnologias digitais favoreceu o surgimento e o aprimoramento dos crimes cibernéticos, fenômeno que passou a demandar maior atenção do sistema jurídico. Observa-se, portanto, o Direito Digital surge como respostas às transformações tecnológicas que passaram a impactar as relações jurídicas contemporâneas.

---

[7] BRASIL. Ministério das Comunicações. Portaria Interministerial nº 147, de 31 de maio de 1995. Disponível em: https://www.cgi.br/portarias/numero/147/. Acesso em: 14 mar. 2026.

[8] SANTOS, Gualtiele Keiber Falcão dos; NASCIMENTO, Emanoel Lourenço do. Aplicação penal dos cibercrimes contra dignidade sexual. Revista FT, 2022. Disponível em: https://revistaft.com.br/aplicacao-penal-dos-cibercrimes-contra-dignidade-sexual/. Acesso em: 12 mar. 2025.

2.2 Conceito e terminologia dos crimes digitais

Os crimes digitais consistem em infrações penais praticadas por meio do uso de tecnologias da informação, como computadores, smartphones e redes de comunicação, ou que tenham como alvo direto sistemas informatizados e dados digitais. Trata-se de condutas ilícitas que se desenvolvem no ambiente virtual ou que dele se utilizam como instrumento para a consecução do resultado criminoso.

Nesse contexto, observa-se que há uma multiplicidade terminológica que reflete a própria complexidade do fenômeno, envolvendo diferentes bens jurídicos, meios de execução e níveis de sofisticação tecnológica. Podem ser utilizadas diversas denominações, como crimes digitais, crimes informáticos ou crimes cibernéticos, dentre outras.

Independentemente da terminologia adotada, é consenso que essas condutas não se desenvolvem à margem do ordenamento jurídico. Ao contrário, quando o meio digital é utilizado como ferramenta para a prática do delito, torna-se plenamente possível o enquadramento das condutas aos tipos penais existentes, respeitadas as particularidades do ambiente virtual.

2.3 Classificação e principais modalidades de crimes digitais

A doutrina majoritária distingue os crimes digitais em próprios (ou puros) e impróprios (ou impuros), classificação que auxilia na compreensão do bem jurídico diretamente atingido e das diferentes formas de manifestação da criminalidade no ambiente virtual.[9]

Os crimes digitais próprios são aqueles em que o sistema informático, o dispositivo eletrônico ou os dados digitais constituem o próprio objeto da conduta criminosa. Nesses casos, o ataque recai diretamente sobre o funcionamento do sistema ou sobre as informações nele armazenadas, comprometendo sua integridade, confidencialidade ou disponibilidade. Exemplos recorrentes incluem a invasão de

[9] SYDOW, Spencer Toth. Curso de Direito Penal Informático. 2 ed. rev. e atual. Salvador: Editora JusPodivm, 2021, p. 271-272.

dispositivos informáticos, a inserção de softwares maliciosos, a interceptação indevida de comunicações eletrônicas e o acesso não autorizado a bancos de dados.

Por sua vez, os crimes digitais impróprios correspondem a ilícitos penais já tradicionalmente previstos no ordenamento jurídico, mas que passaram a ser executados por meio das tecnologias digitais. Nessa hipótese, o ambiente virtual funciona como instrumento para a prática de crimes que já existiam anteriormente, mas que ganharam novas formas de execução com o desenvolvimento das tecnologias da informação. Enquadram-se nessa categoria condutas como estelionato, difamação, ameaça e fraudes diversas praticadas com o auxílio da internet e de ferramentas digitais.

Essa distinção evidencia que a criminalidade no ambiente virtual não se limita à criação de novos tipos penais, mas também envolve a adaptação de condutas ilícitas tradicionais às possibilidades oferecidas pelo meio digital.

A expansão das tecnologias da informação e o uso cada vez mais intenso da internet nas atividades cotidianas contribuíram para o surgimento e a disseminação de diversas modalidades de crimes digitais, que podem apresentar diferentes níveis de complexidade técnica e atingir tanto sistemas informáticos quanto usuários comuns da rede.

Entre as práticas ilícitas mais recorrentes no ambiente digital, destacam-se a: I. A invasão de dispositivos informáticos, caracterizada pelo acesso não autorizado a computadores, redes ou sistemas mediante violação de mecanismos de segurança; II. O roubo e vazamento de dados, que envolve a obtenção ilícita de informações pessoais, financeiras ou estratégicas; III. O phishing, técnica utilizada para induzir a vítima a fornecer dados sensíveis por meio de comunicações fraudulentas que simulam mensagens de instituições legítimas.

Também são frequentes as fraudes financeiras digitais, como clonagem de cartões, transferências indevidas e golpes bancários realizados por meios eletrônicos, bem como práticas de difamação, calúnia e outros crimes contra a honra praticados no ambiente virtual, especialmente por meio de redes sociais e plataformas digitais. Outro exemplo relevante consiste no estelionato virtual, frequentemente observado

em anúncios enganosos, leilões falsos ou falsas oportunidades comerciais divulgadas na internet.

Além disso, observa-se também a divulgação não autorizada de imagens íntimas, consistente no compartilhamento de conteúdo de nudez ou de caráter sexual sem o consentimento da vítima, prática que pode gerar graves violações à dignidade, à privacidade e à imagem das pessoas envolvidas.

Mais recentemente, o desenvolvimento de tecnologias baseadas em inteligência artificial também passou a possibilitar novas formas de manipulação digital, como a criação de imagens, áudios ou vídeos falsificados, utilizados para disseminação de desinformação ou para a prática de fraudes.

A ocorrência dessas práticas evidencia que a criminalidade acompanha as transformações tecnológicas da sociedade, utilizando o ambiente digital tanto como meio quanto como objeto da atividade criminosa. Outrossim, os crimes praticados nesse contexto apresentam particularidades que influenciam diretamente sua forma de execução, bem como os desafios enfrentados pelos mecanismos de prevenção, investigação e repressão penal. Nesse sentido, torna-se relevante examinar as características estruturais desses delitos e os impactos decorrentes de sua prática, aspectos que serão analisados no tópico seguinte.

2.4 Características estruturais dos crimes digitais e seus impactos jurídicos e sociais

Os crimes digitais apresentam características próprias que dificultam sua prevenção, investigação e repressão, especialmente em razão das particularidades do ambiente virtual em que são praticados. Uma das principais características está relacionada ao anonimato, já que a internet possibilita a ocultação da identidade dos agentes por meio do uso de pseudônimos, redes privadas, serviços de redirecionamento de conexão, navegação em redes anônimas e até mesmo pela utilização de transações financeiras descentralizadas. Esse cenário contribui diretamente para a sensação de impunidade, uma vez que a identificação dos

responsáveis se torna mais complexa e, muitas vezes, depende de técnicas investigativas especializadas.

Outro aspecto relevante diz respeito à globalidade e à transnacionalidade dessas infrações. Diferentemente dos crimes tradicionais, os delitos digitais não se submetem a limites territoriais, podendo um único agente atuar em diversas jurisdições simultaneamente. É comum que servidores estejam localizados em países distintos daqueles em que se encontram as vítimas, o que gera dificuldades na definição de competência e exige a utilização de mecanismos de cooperação jurídica internacional, nem sempre ágeis ou eficazes. Essa característica reforça o caráter global da criminalidade digital e evidencia os limites das estruturas jurídicas baseadas em fronteiras territoriais.

Além disso, destaca-se a velocidade com que essas práticas podem ser executadas e o seu alcance em larga escala. No ambiente digital, a propagação de informações ocorre de forma praticamente instantânea, permitindo que um único ataque ou ação criminosa atinja muitas vítimas em um curto espaço de tempo. Muitas dessas condutas, inclusive, podem ser automatizadas, o que potencializa ainda mais seus efeitos e amplia os danos causados.

A complexidade técnica também se apresenta como um fator relevante nesse contexto. Diversas práticas ilícitas no meio digital exigem conhecimentos específicos em áreas como programação, criptografia e segurança da informação, além do uso de técnicas voltadas à ocultação de rastros digitais. Isso não apenas dificulta a investigação por parte das autoridades, mas também exige a atuação de profissionais especializados e o constante aprimoramento dos mecanismos de perícia digital.

Por fim, observa-se que o baixo custo operacional representa um fator que contribui para a expansão dessas práticas. A ampla disponibilidade de ferramentas digitais, muitas vezes acessíveis de forma gratuita ou com baixo investimento, reduz significativamente as barreiras de entrada para a prática criminosa, permitindo que um número maior de indivíduos tenha acesso a meios para a realização de condutas ilícitas no ambiente virtual.

Diante dessas características, percebe-se que o ambiente digital favorece a ampliação dos impactos decorrentes dessas condutas ilícitas. O anonimato, a ausência de barreiras territoriais e a rapidez na disseminação de informações contribuem para a multiplicação das vítimas e dificultam a atuação dos mecanismos tradicionais de investigação e responsabilização penal. Como consequência, os efeitos dos crimes digitais ultrapassam a esfera individual, atingindo dimensões jurídicas, sociais e econômicas mais amplas, o que reforça a necessidade de respostas institucionais cada vez mais estruturadas e eficazes

No plano material, tais ilícitos podem ocasionar prejuízos financeiros significativos, sobretudo em razão de fraudes e estelionatos eletrônicos. Já no âmbito extrapatrimonial, atingem diretamente direitos da personalidade, especialmente a honra, a imagem, a intimidade e a privacidade, frequentemente violados por meio da divulgação indevida de informações e da exposição não autorizada no ambiente virtual.

Sob a perspectiva jurídico-penal, tais práticas não se encontram à margem do ordenamento jurídico. O uso do meio digital como instrumento da conduta ilícita permite o enquadramento nos tipos penais já existentes, previstos no Código Penal Brasileiro e em legislações especiais.

Em dimensão mais ampla, os crimes digitais também afetam a confiança social nas tecnologias, impactam a atividade econômica e podem fragilizar a segurança das instituições, impondo ao Estado o desafio permanente de aprimorar seus mecanismos de prevenção e repressão.

Diante da multiplicidade de condutas ilícitas que podem ser praticadas no ambiente digital, torna-se evidente a necessidade de instrumentos jurídicos capazes de prevenir, investigar e reprimir essas práticas. Nesse sentido, o ordenamento jurídico brasileiro passou a desenvolver mecanismos normativos voltados à regulação do ambiente virtual e à responsabilização de condutas ilícitas, os quais serão analisados no capítulo seguinte.

3. O TRATAMENTO JURÍDICO DOS CRIMES DIGITAIS NO ORDENAMENTO BRASILEIRO

O avanço das tecnologias da informação e a expansão do uso da internet trouxeram benefícios significativos para a sociedade contemporânea, mas também possibilitaram o surgimento de novas formas de criminalidade. Diante desse cenário, o ordenamento jurídico brasileiro passou a incorporar normas destinadas à regulamentação do ambiente digital, à proteção de dados pessoais e à repressão de condutas ilícitas praticadas por meio de tecnologias da informação.

Diversos diplomas legais passaram a compor esse conjunto normativo, formando a base jurídica que orienta a atuação do Estado e dos particulares no espaço virtual. Entre os principais instrumentos legislativos relacionados ao enfrentamento dos crimes digitais destacam-se o Marco Civil da Internet, a Lei Geral de Proteção de Dados e a Lei Carolina Dieckmann, além de outras normas que, embora não tratem exclusivamente da internet, possuem aplicação relevante no ambiente digital.[10]

A análise desses instrumentos jurídicos é fundamental para compreender de que maneira o direito brasileiro busca estruturar mecanismos de prevenção, investigação e responsabilização diante das práticas ilícitas ocorridas no meio virtual.

3.1 Marco Civil da Internet (Lei n°12.965/2014)

O Marco Civil da Internet representa um dos principais marcos normativos do Direito Digital brasileiro, estabelecendo diretrizes para o uso da internet no país. A legislação foi concebida com o objetivo de garantir direitos fundamentais no ambiente

[10] BRASIL. Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 05 abril 2025;
BRASIL. Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 07 abril 2025;
BRASIL. Lei nº 12.737, de 30 de novembro de 2012 (Lei Carolina Dieckmann). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 16 abril 2025.

digital, ao mesmo tempo em que define responsabilidades para usuários, provedores de conexão e provedores de aplicações.

Entre seus princípios centrais destacam-se a garantia da liberdade de expressão, a proteção da privacidade e dos dados pessoais, bem como a inviolabilidade das comunicações realizadas por meio da internet. A norma também consagra o princípio da neutralidade da rede, determinando que os provedores de conexão devem tratar de forma isonômica os dados que trafegam na rede, sem discriminação em razão de conteúdo, origem ou destino.

No âmbito da repressão a ilícitos digitais, a legislação possui relevância ao estabelecer regras relacionadas à guarda e ao fornecimento de registros de conexão e de acesso a aplicações de internet. Esses registros podem ser utilizados como elementos probatórios em investigações criminais, sendo seu acesso condicionado à ordem judicial. Dessa forma, a norma busca equilibrar a necessidade de investigação de condutas ilícitas com a preservação de direitos fundamentais dos usuários.

3.2 Lei Geral de Proteção de Dados – LGPD (Lei n° 13.709/2018)

A Lei Geral de Proteção de Dados consolidou-se como um dos principais instrumentos de proteção da privacidade no ordenamento jurídico brasileiro. A legislação estabelece regras para o tratamento de dados pessoais por pessoas físicas ou jurídicas, tanto no setor público quanto no setor privado.

Entre seus objetivos principais estão a proteção da liberdade, da privacidade e do livre desenvolvimento da personalidade do indivíduo, diante do crescente fluxo de informações pessoais na sociedade digital. Para isso, a norma regula atividades relacionadas à coleta, utilização, armazenamento e compartilhamento de dados pessoais.

A lei também diferencia dados pessoais comuns e dados pessoais sensíveis, estes últimos relacionados a informações que podem gerar discriminação, como dados referentes à saúde, orientação religiosa ou convicções políticas. Tais informações recebem proteção reforçada pela legislação.

Outro aspecto relevante da norma consiste no fortalecimento dos direitos dos titulares de dados, garantindo maior transparência quanto ao tratamento de suas informações e assegurando mecanismos para o exercício de controle sobre esses dados.

A aplicação prática da legislação passou a ser observada logo após sua entrada em vigor. Em setembro de 2020, o Tribunal de Justiça do Estado de São Paulo reconheceu a incidência da LGPD em decisão que condenou uma empresa ao pagamento de indenização por danos morais em razão do uso indevido de dados pessoais para fins de marketing, sem o consentimento do titular.[11] O caso evidenciou a possibilidade de responsabilização jurídica diante do tratamento inadequado de informações pessoais.

Apesar desses avanços, a efetividade da legislação ainda enfrenta desafios relacionados à conscientização da população sobre seus direitos em matéria de proteção de dados. Pesquisa divulgada pela Autoridade Nacional de Proteção de Dados indicou que parcela significativa da população brasileira ainda possui conhecimento limitado sobre o tema, o que demonstra a necessidade de ampliação das políticas de educação digital e de proteção de dados.

3.3 Lei Carolina Dieckmann (Lei n°12.737/2012)

A Lei Carolina Dieckmann representou um importante avanço na tipificação de condutas ilícitas relacionadas ao ambiente digital no ordenamento jurídico brasileiro.

A norma introduziu o artigo 154-A no Código Penal, tipificando o crime de invasão de dispositivo informático alheio com o objetivo de obter, adulterar ou destruir dados sem autorização do titular ou do usuário do dispositivo.[12]

Com essa previsão legal, passaram a ser criminalizadas condutas como a invasão de computadores, smartphones ou outros dispositivos eletrônicos mediante violação de mecanismos de segurança. A legislação também prevê aumento de pena

[11] MIRANDA, Júlia; MARTINEZ, Diego. Decisão do TJ/SP inaugura aplicação da LGPD. Migalhas. Disponível em: https://www.migalhas.com.br/depeso/334657/decisao-do-tj-sp-inaugura-aplicacao-da-lgpd. Acesso em: 20 de maio 2025.
[12] BRASIL. Lei nº 12.737, de 30 de novembro de 2012.

em determinadas circunstâncias, como nos casos em que ocorre divulgação, comercialização ou transmissão das informações obtidas.

A criação desse tipo penal buscou suprir lacuna existente na legislação brasileira, oferecendo instrumentos mais adequados para a repressão de práticas ilícitas relacionadas ao acesso indevido a sistemas informáticos e à violação de dados digitais.

3.4 Outras normas relevantes no combate aos crimes digitais

Além das legislações já mencionadas, outras normas do ordenamento jurídico brasileiro também desempenham papel relevante no enfrentamento dos crimes digitais, ainda que não tenham sido criadas especificamente para esse contexto. Isso demonstra que a regulação do ambiente virtual não depende apenas de leis próprias do Direito Digital, mas também da adaptação de diplomas normativos tradicionais às novas dinâmicas tecnológicas.

Nesse sentido, destaca-se a Lei nº 12.527/2011 (Lei de Acesso à Informação), que assegura o direito fundamental de acesso às informações públicas, inclusive aquelas disponibilizadas em meio digital.[13] Embora não trate diretamente de crimes cibernéticos, essa norma contribui para a transparência da atuação estatal e para o fortalecimento do controle social, aspectos que se mostram relevantes em um contexto em que dados e informações circulam amplamente no ambiente virtual.

Da mesma forma, a Lei nº 9.296/1996 (Lei de Interceptação Telefônica) possui aplicação significativa no âmbito das investigações envolvendo crimes digitais.[14] Essa legislação regulamenta a interceptação de comunicações telefônicas e telemáticas, permitindo sua utilização como meio de obtenção de prova, desde que haja autorização judicial devidamente fundamentada. No contexto digital, sua aplicação tem se expandido para abarcar comunicações realizadas por meio de aplicativos e

[13] BRASIL. Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 04 jun. 2025.
[14] BRASIL. Lei nº 9.296, de 24 de julho de 1996 (Lei de Interceptação Telefônica). Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Acesso em: 04 jun 2025.

outras ferramentas tecnológicas, o que evidencia a necessidade de interpretação evolutiva das normas jurídicas diante das inovações tecnológicas.

Outro diploma de grande relevância é a Lei nº 8.078/1990 (Código de Defesa do Consumidor), cuja incidência no ambiente digital tem se tornado cada vez mais frequente, especialmente nas relações de consumo realizadas por meio do comércio eletrônico.[15] Nesse cenário, a norma atua na proteção dos consumidores contra práticas abusivas, fraudes, publicidade enganosa e falhas na prestação de serviços digitais, impondo responsabilidade aos fornecedores e contribuindo para a segurança das transações realizadas no meio virtual.

Além disso, merece destaque a Lei nº 14.155/2021, que promoveu alterações no Código Penal brasileiro com o objetivo de tornar mais rigorosa a repressão a determinadas práticas criminosas realizadas no ambiente digital.[16] Essa legislação introduziu qualificadoras e causas de aumento de pena para crimes de furto mediante fraude cometidos por meio de dispositivos eletrônicos ou informáticos, com especial atenção às situações que envolvem vítimas idosas ou em condição de vulnerabilidade. Trata-se de uma resposta legislativa direta ao aumento das fraudes eletrônicas, especialmente aquelas praticadas por meio de aplicativos de mensagens e plataformas digitais.

A presença desses instrumentos normativos evidencia que o ordenamento jurídico brasileiro tem buscado, de forma progressiva, incorporar mecanismos voltados à regulação do ambiente digital e ao enfrentamento das práticas ilícitas nele desenvolvidas. No entanto, é importante destacar que a simples existência dessas normas não garante, por si só, a plena efetividade da proteção jurídica no espaço virtual. A aplicação concreta dessas disposições depende de fatores como a atuação eficiente dos órgãos de investigação, a capacitação técnica dos profissionais envolvidos e a adaptação das instituições às novas realidades tecnológicas.

Diante disso, torna-se fundamental analisar de que maneira essas normas vêm sendo aplicadas na prática, bem como identificar os principais obstáculos enfrentados

[15] BRASIL. Lei nº 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor). Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078.htm . Acesso em: 22 maio 2025.
[16] BRASIL. Lei nº 14.155, de 27 de maio de 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm. Acesso em: 12 jun. 2025.

pelo sistema jurídico brasileiro na investigação e repressão dos crimes digitais. Entre esses desafios, destacam-se a complexidade técnica das condutas, a dificuldade na obtenção de provas digitais e a necessidade de cooperação entre diferentes jurisdições, elementos que serão abordados nos tópicos seguintes.

4. UMA ANÁLISE DO SISTEMA JURÍDICO BRASILEIRO NO ENFRENTAMENTO AOS CRIMES DIGITAIS

A existência de instrumentos normativos voltados à regulação do ambiente digital demonstra que o ordenamento jurídico brasileiro tem buscado responder aos desafios impostos pela crescente incidência de crimes praticados por meio das tecnologias da informação. Contudo, a simples previsão de normas jurídicas não garante, por si só, a plena eficácia na prevenção e repressão dessas condutas ilícitas.

O enfrentamento dos crimes digitais envolve uma série de fatores que ultrapassam a dimensão meramente legislativa, abrangendo também aspectos institucionais, estruturais e tecnológicos que influenciam diretamente a atuação dos órgãos responsáveis pela investigação, persecução penal e julgamento dessas infrações. Nessa condição, torna-se necessário analisar de forma crítica o funcionamento do sistema jurídico brasileiro diante das novas dinâmicas da criminalidade digital.

Assim, o presente capítulo busca examinar as principais limitações e desafios enfrentados pelo ordenamento jurídico nacional no combate aos crimes digitais, bem como identificar avanços normativos e institucionais relevantes nesse processo.

4.1 Limitações estruturais e investigativas do sistema jurídico brasileiro

O crescimento expressivo dos crimes praticados no ambiente digital nas últimas décadas tem imposto novos desafios ao sistema de justiça criminal brasileiro. A expansão do uso da internet, associada à crescente digitalização das relações sociais, econômicas e institucionais, ampliou significativamente as possibilidades de prática de ilícitos no ambiente virtual. Nesse contexto da análise do sistema jurídico brasileiro no enfrentamento aos crimes digitais encontra limitações estruturais relevantes, especialmente no que se refere à capacidade investigativa e à especialização institucional.

No âmbito do Poder Judiciário, não existem, de forma ampla, tribunais ou varas especializadas exclusivamente voltadas ao julgamento de crimes digitais. Em razão disso, tais delitos são, em regra, apreciados por varas criminais comuns, cujos

magistrados nem sempre dispõem de formação técnica específica para lidar com questões envolvendo provas digitais, perícias informáticas e condutas praticadas em ambientes virtuais de elevada complexidade tecnológica.

No campo investigativo, o cenário revela desafios ainda mais significativos. O número de delegacias especializadas em repressão a crimes cibernéticos no Brasil permanece reduzido diante da dimensão territorial do país, da quantidade de usuários da internet e do crescimento contínuo das infrações praticadas no ambiente digital. De acordo com levantamento divulgado pela SaferNet Brasil, existem atualmente apenas 18 delegacias especializadas em crimes cibernéticos no território nacional, número considerado insuficiente para atender à demanda crescente por investigações dessa natureza.[17]

Essa limitação estrutural compromete a celeridade das investigações, dificulta a adequada coleta e preservação de provas digitais e contribui para a sensação de impunidade associada a determinadas práticas ilícitas no ambiente virtual. Embora existam iniciativas relevantes em alguns estados, como a 4ª Delegacia de Delitos Cometidos por Meios Eletrônicos (DIG/DEIC) do Estado de São Paulo, dedicada à investigação de crimes praticados por meio da internet, tais estruturas ainda são pontuais e não se encontram uniformemente distribuídas pelo país.[18]

De modo geral, a investigação de crimes digitais no Brasil é conduzida principalmente pela Polícia Civil, por meio de delegacias especializadas ou unidades comuns; pela Polícia Federal, especialmente nos casos que envolvem crimes interestaduais, organizações criminosas ou infrações com repercussão internacional; e pelo Ministério Público, que pode atuar tanto na instauração de procedimentos investigatórios quanto na condução da persecução penal.

Apesar da atuação dessas instituições, a resposta estatal ainda enfrenta obstáculos significativos. A escassez de recursos humanos e tecnológicos, aliada à complexidade técnica das investigações envolvendo sistemas informáticos, redes

[17] SAFERNET BRASIL. Delegacias especializadas em crimes cibernéticos no Brasil. Disponível em: https://new.safernet.org.br/content/delegacias-cibercrimes. Acesso em: 14 mar. 2026.
[18] SAFERNET BRASIL. Delegacias especializadas em crimes cibernéticos no Brasil. Disponível em: https://new.safernet.org.br/content/delegacias-cibercrimes. Acesso em: 14 mar. 2026.

digitais e análise de dados, dificulta a atuação eficiente dos órgãos responsáveis pela repressão a essas condutas ilícitas.

Outro fator relevante diz respeito à dimensão transnacional dos crimes digitais. Em muitos casos, as infrações são praticadas por meio de servidores localizados em outros países ou mediante o uso de mecanismos de anonimização, como redes privadas, criptografia e criptomoedas, o que torna indispensável a cooperação internacional para a identificação dos autores e a obtenção de provas digitais. Nessa esfera, destaca-se, no plano internacional, a Convenção de Budapeste sobre o Cibercrime, instrumento que busca harmonizar legislações e fortalecer a cooperação entre Estados no enfrentamento da criminalidade digital.[19]

Outrossim, a ausência de programas contínuos de capacitação técnica para agentes públicos também constitui um desafio relevante. A investigação de crimes digitais exige conhecimentos especializados em tecnologia da informação, segurança cibernética e análise forense de dados, competências que nem sempre estão disponíveis de forma homogênea nos órgãos de segurança pública. Nesse sentido, é necessário ressaltar que o enfrentamento eficaz dos crimes cibernéticos depende não apenas da existência de normas jurídicas adequadas, mas também da presença de profissionais capacitados e de estruturas institucionais aptas a investigar e processar tais delitos.

Dessa forma, embora o Brasil possua avanços normativos relevantes no campo do Direito Digital, as limitações estruturais do sistema de justiça criminal, especialmente a insuficiência de delegacias especializadas, a carência de recursos tecnológicos e a necessidade de constante capacitação técnica, ainda representam entraves concretos à atuação do sistema jurídico no enfrentamento aos crimes digitais, evidenciando a necessidade de investimentos institucionais, capacitação técnica contínua e desenvolvimento de políticas públicas voltadas ao fortalecimento das estruturas investigativas e judiciais no enfrentamento da criminalidade digital.

[19] CONSELHO DA EUROPA. Convenção sobre o Cibercrime (Convenção de Budapeste). Budapeste, 23 de novembro de 2001. Série de Tratados do Conselho da Europa, nº 185. Disponível em: https://www.coe.int. Acesso em: 21 set. 2025.

4.2 Lacunas legislativas e insegurança jurídica

A análise do sistema jurídico brasileiro no enfrentamento aos crimes digitais revela a existência de lacunas legislativas e dificuldades interpretativas que contribuem para a formação de um cenário de insegurança jurídica. Embora o Poder Judiciário venha construindo uma jurisprudência relevante sobre delitos praticados no ambiente virtual, ainda não se verifica plena uniformidade nos entendimentos, o que pode gerar divergências na aplicação do direito.

Grande parte dos tipos penais atualmente utilizados para reprimir condutas praticadas na internet foi concebida em momento anterior à ampla difusão das tecnologias digitais. Em razão disso, diversas práticas ilícitas ocorridas no ambiente virtual acabam sendo enquadradas por meio de interpretação extensiva ou adaptação de tipos penais originalmente destinados a situações do mundo físico. Embora tais interpretações sejam juridicamente possíveis em determinados casos, nem sempre conseguem abranger de maneira satisfatória as especificidades das condutas praticadas no ciberespaço, especialmente diante das exigências impostas pelo princípio da legalidade penal.

A omissão legislativa também se apresenta como um fator relevante nesse contexto. Em diversas situações, crimes praticados no ambiente digital, sobretudo aqueles relacionados à honra ou à exposição indevida de informações pessoais, acabam situando-se em uma espécie de zona de incerteza normativa, decorrente da dificuldade do legislador em acompanhar, com a mesma velocidade, as transformações tecnológicas e comportamentais da sociedade contemporânea.[20]

Nesse cenário, projetos de lei em tramitação no Congresso Nacional buscam suprir algumas dessas lacunas, especialmente no que se refere à tipificação de condutas como a extorsão digital, o sequestro de dados e outras práticas ilícitas associadas à criminalidade informática. Entretanto, o processo legislativo possui dinâmica própria e demanda tempo para a discussão, aprovação e implementação

[20] SILVA, Stephane Kamily de Oliveira; ANDRADE, Felipe de. A evolução dos crimes cibernéticos e os desafios da legislação brasileira. Revista FT, 2022. Disponível em: https://revistaft.com.br/a-evolucao-dos-crimes-ciberneticos-e-os-desafios-da-legislacao-brasileira/. Acesso em: 11 jun 2025.

das normas, o que faz com que, muitas vezes, a evolução tecnológica avance de maneira mais acelerada do que a produção legislativa.

A experiência internacional demonstra que esse desafio não é exclusivo do ordenamento jurídico brasileiro. Diversos países têm buscado desenvolver mecanismos regulatórios capazes de acompanhar as transformações do ambiente digital. Nesse contexto, destaca-se a aprovação, pela União Europeia, do Digital Services Act, que estabelece obrigações mais rigorosas às plataformas digitais quanto à remoção de conteúdos ilegais, à transparência nos processos de moderação e à mitigação de riscos associados à disseminação de conteúdos ilícitos no ambiente virtual. Iniciativas dessa natureza evidenciam a crescente preocupação internacional com a construção de instrumentos jurídicos capazes de lidar com as novas dinâmicas do ciberespaço.[21]

Diante dessa realidade dinâmica, parte da doutrina sustenta que normas excessivamente específicas tendem a tornar-se rapidamente obsoletas diante da velocidade das transformações tecnológicas. Assim, normas com maior grau de generalidade e caráter principiológico podem apresentar maior capacidade de adaptação às novas formas de interação social e às diferentes modalidades de condutas ilícitas que surgem no ambiente digital.

Além das dificuldades normativas, também se observa um fator comportamental relevante no ciberespaço. Muitas pessoas, ao se conectarem ao ambiente virtual, experimentam uma sensação ilusória de anonimato ou liberdade absoluta, acreditando não estarem submetidas às mesmas normas jurídicas, éticas e sociais que regem o convívio no mundo físico. Esse fenômeno não se restringe apenas aos agentes que praticam condutas ilícitas, mas também pode atingir as próprias vítimas, que frequentemente desconhecem ou subestimam os riscos presentes nas interações digitais.[22]

---

[21] UNIÃO EUROPEIA. Regulamento (UE) 2022/2065 do Parlamento Europeu e do Conselho, de 19 de outubro de 2022 (Digital Services Act – DSA). Disponível em: https://eur-lex.europa.eu. Acesso em: 10 jan. 2026.

[22] BARRETO, Alesandro Gonçalves; BRASIL, Beatriz Silveira. Manual de Investigação Cibernética: à luz do Marco Civil da Internet. Rio de Janeiro: Brasport, 2016, p. 189.

Deste modo, a existência de lacunas legislativas, aliada à constante evolução tecnológica e à ausência de uniformidade jurisprudencial em determinados temas, contribui para um cenário de insegurança jurídica no tratamento dos crimes digitais. Tal contexto evidencia a necessidade de contínuo aprimoramento legislativo, bem como do desenvolvimento de interpretações jurídicas capazes de acompanhar a complexidade das relações estabelecidas no ambiente digital.

4.3 Inteligência artificial e novos desafios à responsabilização jurídica

A incorporação da inteligência artificial às práticas criminosas acrescenta novos níveis de complexidade ao enfrentamento jurídico dos crimes digitais. Sistemas baseados em inteligência artificial são capazes de automatizar ataques, aperfeiçoar técnicas de fraude e dificultar a identificação de seus responsáveis, o que desafia os modelos tradicionais de investigação e de imputação de responsabilidade no âmbito civil e penal.

A evolução dessas tecnologias tem contribuído para o aumento da sofisticação dos ataques cibernéticos. Dados recentes indicam que o Brasil ocupa posição de destaque no cenário global de ataques digitais, registrando mais de 700 milhões de ataques cibernéticos em um período de doze meses, o que corresponde a aproximadamente 1.379 tentativas por minuto. Especialistas em cibersegurança apontam que o avanço da inteligência artificial tem desempenhado papel relevante nesse cenário, possibilitando a criação de golpes mais complexos e difíceis de detectar, como fraudes baseadas em simulação de voz, nas quais criminosos utilizam tecnologias capazes de reproduzir a fala de autoridades, celebridades ou até mesmo familiares das vítimas (CNN BRASIL, 2024).[23] Entre essas práticas, destacam-se também os chamados deepfakes, conteúdos audiovisuais manipulados por inteligência artificial que podem ser utilizados para disseminação de desinformação, fraudes ou ataques à reputação de indivíduos.

[23] CNN BRASIL. País tem 700 milhões de ataques virtuais em um ano, diz relatório. Disponível em: https://www.cnnbrasil.com.br/economia/negocios/pais-tem-700-milhoes-de-ataques-virtuais-em-um-ano-diz-relatorio/. Acesso em: 19 nov. 2025.

Desse modo, observa-se que a inteligência artificial apresenta simultaneamente oportunidades e desafios para o Direito. A capacidade desses sistemas de aprender, adaptar-se e executar tarefas com elevado grau de autonomia suscita questionamentos relevantes sobre responsabilidade jurídica, ética e regulamentação. Operadores do direito, legisladores e pesquisadores passam a enfrentar o desafio de compreender de que maneira as normas jurídicas existentes podem ser aplicadas a essas novas tecnologias, bem como se mostram necessárias adaptações normativas para lidar com os novos cenários decorrentes da transformação digital.

Um dos principais debates jurídicos relacionados à inteligência artificial refere-se à atribuição de responsabilidade civil e penal pelos danos eventualmente causados por sistemas automatizados. Surge, desta forma, a discussão acerca de quem deve responder juridicamente por tais condutas: o desenvolvedor do software, o proprietário do sistema, o usuário que o utiliza ou, em hipóteses mais controversas, a própria inteligência artificial enquanto entidade autônoma.

No atual estágio do ordenamento jurídico, contudo, a inteligência artificial não pode ser considerada sujeito de direito nem ser responsabilizada de forma autônoma, uma vez que não possui personalidade jurídica. Dessa forma, a responsabilização tende a recair sobre pessoas físicas ou jurídicas envolvidas no desenvolvimento, na disponibilização ou na utilização do sistema. Ainda assim, a identificação do responsável nem sempre é simples, especialmente em situações nas quais os algoritmos apresentam elevado grau de autonomia operacional.

No cenário internacional, observa-se crescente preocupação com a necessidade de estabelecer parâmetros regulatórios para o desenvolvimento e a utilização da inteligência artificial. Nesse sentido, destaca-se a aprovação, pela União Europeia, da Lei de Inteligência Artificial (do inglês, Artificial Intelligence Act), considerado um dos primeiros marcos regulatórios abrangentes voltados especificamente à inteligência artificial.[24] A norma estabelece diretrizes para o

[24] JOTA. UE é pioneira na regulamentação de sistemas de inteligência artificial. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/regula-euro/ue-e-pioneira-na-regulamentacao-de-sistemas-de-inteligencia-artificial. Acesso em: 11 jan. 2026.

desenvolvimento, utilização e controle de sistemas baseados em IA classificando aplicações conforme o nível de risco e impondo obrigações mais rigorosas para tecnologias potencialmente mais perigosas.

Diante desse panorama, o avanço da inteligência artificial no ambiente digital evidencia novos desafios para o Direito. A complexidade dessas tecnologias exige constante reflexão jurídica e atualização normativa, de modo a permitir que o ordenamento jurídico acompanhe as transformações tecnológicas e seja capaz de oferecer respostas adequadas às novas formas de criminalidade que emergem no contexto da sociedade digital.

4.4 Normas de segurança da informação e proteção de dados

A análise do enfrentamento aos crimes digitais no ordenamento jurídico brasileiro não se limita à atuação jurisdicional ou à aplicação direta de normas penais, envolvendo também um conjunto de instrumentos normativos voltados à segurança da informação, à prevenção de incidentes cibernéticos e à proteção de dados pessoais.

Sob essa perspectiva, destaca-se a Estratégia Nacional de Cibersegurança (E-Ciber), originalmente instituída pelo Decreto nº 10.222/2020 e recentemente atualizada pelo Decreto nº 12.573/2025.[25] A nova norma, que revogou o diploma anterior, estabelece diretrizes robustas para o fortalecimento da segurança digital. Essa atualização normativa reafirma a importância do ciberespaço para a soberania do país. Ao priorizar a proteção de dados e sistemas essenciais, o novo decreto estabelece parâmetros de governança que elevam o nível de maturidade da cibersegurança brasileira no país, incentivando a cooperação entre Estado, setor privado e sociedade civil.

Em complemento, o Decreto nº 10.748/2021 instituiu a Rede Federal de Gestão de Incidentes Cibernéticos, com o objetivo de integrar órgãos e entidades da

[25] BRASIL. Decreto nº 12.573, de 4 de agosto de 2025. Aprova a Estratégia Nacional de Cibersegurança (E-Ciber). Brasília, DF: Presidência da República, 2025. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/decreto/d12375.htm. Acesso em: 21 fev. 2026.

administração pública federal na prevenção, detecção e resposta a ataques cibernéticos.[26] A norma evidencia a preocupação do Estado brasileiro em estruturar mecanismos coordenados de reação a ameaças digitais, especialmente aquelas que possam comprometer serviços públicos essenciais ou envolver o tratamento de dados sensíveis.

No âmbito da proteção de dados pessoais, destaca-se também o papel desempenhado pela Lei Geral de Proteção de Dados Pessoais, que estabelece regras para o tratamento de dados pessoais por pessoas físicas e jurídicas, tanto no setor público quanto no privado. A legislação busca assegurar maior controle aos titulares sobre suas informações pessoais, além de impor deveres de transparência, segurança e responsabilidade aos agentes responsáveis pelo tratamento de dados.

Nesse contexto, a Lei nº 14.460/2022 promoveu alterações relevantes ao transformar a Autoridade Nacional de Proteção de Dados (ANPD) em autarquia de natureza especial.[27] A mudança conferiu maior autonomia administrativa e técnica ao órgão regulador, fortalecendo sua capacidade de fiscalização e regulamentação no âmbito da proteção de dados pessoais.

No cenário internacional, a proteção de dados também tem recebido atenção crescente por parte dos ordenamentos jurídicos. Um dos principais marcos regulatórios nessa área é o Regulamento Geral da Proteção de Dados (do inglês, General Data Protection Regulation), adotado pela União Europeia, que estabelece regras rigorosas para o tratamento de dados pessoais e impõe obrigações significativas às organizações responsáveis por tais atividades.[28] O modelo europeu influenciou diretamente diversas legislações ao redor do mundo, inclusive a estrutura normativa adotada no Brasil com a promulgação da LGPD.

---

[26] BRASIL. Decreto nº 10.748, de 14 de julho de 2021. Institui a Rede Federal de Gestão de Incidentes Cibernéticos. Brasília, DF: Presidência da República, 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/decreto/d10748.htm Acesso em: 02 dez. 2025.

[27] BRASIL. Lei nº 14.460, de 25 de outubro de 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/lei/L14460.htm . Acesso em: 21 nov. 2025.

[28] UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (General Data Protection Regulation – GDPR). Disponível em: https://eur-lex.europa.eu. Acesso em: 11 jan.. 2026.

Dessa maneira, observa-se que o enfrentamento aos desafios relacionados à criminalidade digital envolve não apenas instrumentos de natureza penal, mas também políticas públicas e estruturas normativas voltadas à segurança da informação e à proteção de dados. Tais mecanismos contribuem para a construção de um ambiente digital mais seguro e para o fortalecimento das estruturas institucionais responsáveis pela prevenção e tratamento de incidentes cibernéticos no contexto brasileiro.

4.5 Avanços normativos e institucionais: atuação do STJ e STF

Após a análise das normas jurídicas voltadas ao enfrentamento dos crimes digitais no ordenamento brasileiro, torna-se relevante examinar como tais dispositivos vêm sendo interpretados e aplicados pelo Poder Judiciário, especialmente pelos tribunais superiores responsáveis pela uniformização da jurisprudência nacional.

Nas últimas décadas, o Brasil passou a reconhecer de forma mais expressiva a necessidade de regulamentar condutas praticadas no ambiente digital. A promulgação de normas como o Marco Civil da Internet, a Lei Geral de Proteção de Dados Pessoais e a Lei Carolina Dieckmann evidenciam o esforço do legislador em criar instrumentos jurídicos voltados à proteção da privacidade, da segurança da informação e à repressão de condutas ilícitas praticadas por meio eletrônico.

Nesse cenário, o aumento de conflitos decorrentes do uso da internet e das tecnologias digitais também levou diversas controvérsias ao Poder Judiciário. Os tribunais superiores brasileiros, especialmente o Superior Tribunal de Justiça, e o órgão máximo, Supremo Tribunal Federal, têm desempenhado papel relevante na interpretação e aplicação das normas relacionadas ao ambiente digital, contribuindo para a construção de parâmetros jurídicos voltados à regulação das relações ocorridas no ciberespaço.

Como tribunal responsável pela uniformização da interpretação da legislação infraconstitucional, o Superior Tribunal de Justiça tem sido constantemente provocado a enfrentar controvérsias relacionadas ao ambiente digital, especialmente no que diz respeito à responsabilidade civil na internet, à atuação de provedores de serviços e à validade das provas digitais no processo penal. Nesse contexto, a Corte vem

demonstrando preocupação não apenas com a aplicação das normas existentes, mas também com a adaptação dos institutos tradicionais às novas dinâmicas tecnológicas.

Um ponto que merece destaque na jurisprudência do STJ diz respeito à validade e à confiabilidade das provas digitais. No julgamento do AgRg no RHC nº 143.169/RJ, a Corte enfrentou discussão relevante acerca da cadeia de custódia de dados informáticos, reconhecendo que a ausência de procedimentos técnicos adequados na coleta, armazenamento e análise de dispositivos eletrônicos compromete a integridade da prova, podendo levar à sua inadmissibilidade.[29]

Na ocasião, o Tribunal ressaltou que, em se tratando de provas digitais, é indispensável a adoção de técnicas específicas, como a extração integral dos dados (cópia “bit a bit”) e a utilização de mecanismos de verificação, como algoritmos hash, capazes de garantir que o conteúdo analisado permaneça íntegro ao longo da investigação. A decisão evidencia que, no contexto da criminalidade digital, a observância rigorosa da cadeia de custódia assume papel ainda mais relevante, tendo em vista a facilidade de alteração e manipulação de dados eletrônicos.

No âmbito constitucional, destaca-se a atuação do Supremo Tribunal Federal na análise de conflitos envolvendo direitos fundamentais no ambiente digital, como liberdade de expressão, privacidade, proteção de dados e segurança pública. Como guardião da Constituição, o STF tem sido chamado a estabelecer parâmetros interpretativos que orientam a atuação estatal e delimitam os limites da intervenção no espaço virtual.

Um dos casos mais emblemáticos enfrentados pela Corte refere-se à possibilidade de bloqueio de aplicações de comunicação amplamente utilizadas. Ao analisar controvérsias envolvendo a suspensão do aplicativo WhatsApp por descumprimento de ordens judiciais, o STF sinalizou que medidas dessa natureza podem configurar restrições desproporcionais à liberdade de comunicação e ao

[29] BRASIL. Superior Tribunal de Justiça. Agravo Regimental no Recurso em Habeas Corpus nº 143.169/RJ. Relator: Jesuíno Rissato (Desembargador convocado). Relator para acórdão: Ribeiro Dantas. Brasília, DF, julgamento em 07 fev. 2023. Diário da Justiça eletrônico, 02 mar. 2023. Disponível em: https://processo.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202100573956&dt_publicacao=02/03/2023. Acesso em: 03 fev. 2026.

acesso à informação, evidenciando a necessidade de ponderação entre a eficácia da persecução penal e a preservação de direitos fundamentais.[30]

Além dessas discussões, o STF também tem enfrentado casos envolvendo a repressão a organizações criminosas que utilizam o ambiente digital para a prática de fraudes em larga escala. Nesse sentido, destaca-se o Habeas Corpus nº 204.808/SP, no qual a Corte manteve a prisão preventiva de investigados acusados de integrar organização criminosa voltada à prática reiterada de estelionatos por meio da internet.[31]

No referido caso, verificou-se a existência de um esquema estruturado que utilizava plataformas digitais e anúncios para atrair consumidores com ofertas fraudulentas, causando prejuízos milionários a muitas vítimas. O STF entendeu que a gravidade concreta das condutas, aliada ao risco de reiteração delitiva, justificava a manutenção da prisão preventiva como forma de garantia da ordem pública, demonstrando que os instrumentos tradicionais do direito penal continuam sendo aplicáveis, ainda que diante de novas formas de criminalidade.

Outro ponto relevante diz respeito à atuação da própria Corte na investigação de práticas ilícitas no ambiente digital. O Inquérito nº 4.781, instaurado para apurar a disseminação de desinformação e ataques às instituições democráticas, evidencia uma preocupação crescente com o uso abusivo das plataformas digitais. Nesse contexto, o STF tem buscado estabelecer limites à liberdade de expressão quando utilizada como instrumento para a prática de ilícitos, reforçando a necessidade de responsabilização no ambiente virtual.[32]

Diante desse panorama, observa-se que tanto o STF quanto o STJ vêm desempenhando papel fundamental na construção de parâmetros jurídicos aplicáveis ao ambiente digital. Suas decisões demonstram um esforço contínuo de adaptação

---

[30] BRASIL. Supremo Tribunal Federal. Arguição de Descumprimento de Preceito Fundamental nº 403. Relator: Edson Fachin. Brasília, DF, 2016. Disponível em: https://www.stf.jus.br/arquivo/cms/bibliotecaConsultaProdutoBibliotecaPastaFachin/anexo/ADPF403voto.pdf. Acesso em: 09 fev. 2026.

[31] BRASIL. Supremo Tribunal Federal. Habeas Corpus nº 204.808/SP. Relator: Alexandre de Moraes. Brasília, DF, 2021. Disponível em: https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/hc204808.pdf. Acesso em: 02 mar. 2026.

[32] BRASIL. Supremo Tribunal Federal. Inquérito nº 4.781/DF. Relator: Alexandre de Moraes. Brasília, DF, 2019. Disponível em: https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/mandado27maio.pdf
. Acesso em: 04 mar. 2026.

do Direito às transformações tecnológicas, especialmente no que se refere à validade das provas digitais, à responsabilização de agentes e à proteção de direitos fundamentais. Ao mesmo tempo, revelam que a efetividade da resposta estatal depende não apenas da existência de normas, mas também da capacidade institucional de interpretá-las e aplicá-las de forma adequada às especificidades da sociedade digital.

4.6 Síntese crítica do sistema jurídico brasileiro aos crimes digitais e perspectivas diante das transformações tecnológicas

A análise do arcabouço normativo brasileiro e da atuação do Poder Judiciário no enfrentamento aos crimes digitais evidencia a crescente preocupação do ordenamento jurídico em responder às transformações decorrentes do avanço das tecnologias da informação. Nesse contexto, observa-se que a construção do Direito Digital no Brasil tem ocorrido de forma progressiva, por meio da criação de normas específicas e da interpretação judicial voltada à adaptação de institutos jurídicos tradicionais às novas dinâmicas das relações estabelecidas no ambiente virtual.

As decisões proferidas pelos tribunais superiores revelam um esforço progressivo de adaptação do Direito às transformações tecnológicas, especialmente diante de questões complexas relacionadas à responsabilização das plataformas digitais, à utilização de provas eletrônicas, à proteção da privacidade e aos limites da liberdade de expressão no ambiente virtual. Contudo, também evidenciam desafios relevantes decorrentes da natureza transnacional da internet, sobretudo no que se refere à obtenção de dados armazenados no exterior, aos mecanismos de cooperação jurídica internacional e às limitações investigativas enfrentadas pelas autoridades competentes, fatores que impactam diretamente a efetividade da persecução penal e da tutela de direitos no meio digital.

Paralelamente, a consolidação de normas voltadas à segurança cibernética e à proteção de dados pessoais demonstra uma tentativa do Estado brasileiro de estruturar respostas institucionais mais amplas aos riscos inerentes ao ambiente digital. A formulação de estratégias nacionais, a criação de redes de gestão de incidentes e o fortalecimento de órgãos reguladores indicam avanços relevantes

nesse campo, ainda que a implementação prática dessas iniciativas enfrente limitações de natureza técnica, estrutural e orçamentária.

Além disso, o rápido desenvolvimento de tecnologias baseadas em inteligência artificial introduz novos desafios ao sistema jurídico, uma vez que tais ferramentas podem ser utilizadas para potencializar práticas ilícitas, automatizar fraudes e dificultar a identificação de seus responsáveis, exigindo do Direito constante atualização interpretativa e normativa para acompanhar essas novas dinâmicas tecnológicas.

Diante desse cenário, observa-se que o sistema jurídico brasileiro no enfrentamento aos crimes digitais apresenta caráter dinâmico e progressivo. Embora o ordenamento jurídico disponha de instrumentos normativos e jurisprudenciais capazes de oferecer respostas relevantes às novas formas de criminalidade digital, persistem entraves institucionais, investigativos e tecnológicos que dificultam sua aplicação uniforme e célere. Assim, o desenvolvimento do Direito Digital no Brasil revela avanços significativos, mas ainda demanda constante aprimoramento para acompanhar, de maneira eficaz, a complexidade e a velocidade das transformações tecnológicas contemporâneas.

Nesse enquadramento, o futuro do Direito Digital no país exige não apenas a atualização normativa, mas também o fortalecimento das estruturas institucionais responsáveis pela prevenção, investigação e repressão de ilícitos praticados no ambiente virtual. A complexidade das investigações digitais, muitas vezes marcadas pela atuação transnacional dos agentes e pela utilização de tecnologias avançadas, demanda maior integração entre instituições públicas, aprimoramento dos mecanismos de cooperação jurídica internacional e investimento contínuo em capacitação técnica dos profissionais que atuam no sistema de justiça.

Adicionalmente, o avanço acelerado de tecnologias emergentes, especialmente aquelas baseadas em inteligência artificial e análise massiva de dados, tende a ampliar os desafios regulatórios enfrentados pelo Direito. Nesse cenário, torna-se fundamental que o ordenamento jurídico brasileiro desenvolva respostas normativas e interpretativas capazes de equilibrar a promoção da inovação tecnológica com a proteção de direitos fundamentais, garantindo que o progresso

tecnológico ocorra em consonância com os princípios jurídicos que orientam o Estado Democrático de Direito.

5. CONCLUSÃO

O desenvolvimento das tecnologias digitais nas últimas décadas trouxe mudanças significativas para a forma como a sociedade se organiza, se comunica e realiza suas atividades cotidianas. A internet passou a ocupar um espaço central nas relações sociais, econômicas e institucionais, ampliando possibilidades de interação e acesso à informação. No entanto, esse mesmo ambiente também passou a ser utilizado para a prática de diversas condutas ilícitas, o que fez surgir novos desafios para o Direito e para as instituições responsáveis pela aplicação da lei.

Ao longo deste trabalho, buscou-se analisar de qual forma o sistema jurídico brasileiro tem procurado responder às práticas criminosas ocorridas no ambiente digital. Observou-se que, nas últimas décadas, o ordenamento jurídico nacional passou por um processo gradual de adaptação, com a criação de normas específicas voltadas à regulamentação da internet e à proteção de direitos no ambiente digital. Nesse contexto, iniciativas legislativas como o Marco Civil da Internet, a Lei Carolina Dieckmann e a Lei Geral de Proteção de Dados Pessoais representam marcos importantes na construção de um conjunto normativo voltado à disciplina das relações digitais e ao enfrentamento de determinadas condutas ilícitas praticadas por meio da internet.

Além da atuação legislativa, também se verificou a importância do papel desempenhado pelo Poder Judiciário na interpretação e aplicação dessas normas. As decisões proferidas pelos tribunais, especialmente em questões relacionadas à responsabilidade de provedores, à utilização de provas digitais e à proteção de dados pessoais, demonstram um esforço progressivo de adaptação do Direito às novas realidades tecnológicas. Esse processo interpretativo tem sido fundamental para suprir lacunas normativas e para estabelecer parâmetros jurídicos aplicáveis a situações que, muitas vezes, não foram originalmente previstas pelo legislador.

Apesar desses avanços, a análise realizada ao longo do trabalho também evidencia que o enfrentamento dos crimes digitais ainda apresenta desafios relevantes. A própria natureza da internet, marcada pela rapidez das transformações tecnológicas e pela circulação global de informações, pode dificultar tanto a

investigação quanto a responsabilização de determinadas condutas ilícitas. Questões como a localização de dados armazenados em servidores estrangeiros, a identificação de usuários responsáveis por práticas criminosas e a necessidade de cooperação internacional são fatores que frequentemente impactam a efetividade das medidas jurídicas adotadas.

Outro aspecto importante diz respeito ao constante surgimento de novas tecnologias, que podem ser utilizadas tanto para fins legítimos quanto para a prática de atividades ilícitas. Ferramentas baseadas em automação, inteligência artificial e análise massiva de dados têm ampliado as possibilidades de atuação no ambiente digital, mas também podem ser exploradas por agentes mal-intencionados para a realização de fraudes, manipulação de informações e outras práticas prejudiciais. Esse cenário exige que o Direito permaneça em constante processo de atualização, buscando acompanhar as mudanças tecnológicas sem comprometer a segurança jurídica.

Diante desse contexto, torna-se evidente que o enfrentamento da criminalidade digital não depende apenas da existência de normas jurídicas específicas, mas também da capacidade das instituições de aplicar essas normas de forma adequada e eficiente. A atuação coordenada entre órgãos de investigação, instituições judiciais e entidades responsáveis pela regulação do ambiente digital mostra-se essencial para a construção de respostas mais eficazes diante das novas formas de criminalidade que surgem no meio virtual.

Adicionalmente, o fortalecimento de estruturas especializadas, o investimento em capacitação técnica dos profissionais que atuam no sistema de justiça e o desenvolvimento de mecanismos de cooperação internacional são fatores que podem contribuir para aprimorar a atuação estatal nesse campo. Ao mesmo tempo, a conscientização da sociedade acerca dos riscos presentes no ambiente digital também desempenha papel relevante na prevenção de determinadas práticas ilícitas.

Dessa forma, pode-se concluir que o sistema jurídico brasileiro tem apresentado avanços importantes no enfrentamento dos crimes digitais,

especialmente no que se refere à construção de um arcabouço normativo voltado à regulamentação da internet e à proteção de direitos no ambiente digital. Contudo, as constantes transformações tecnológicas e a complexidade das relações estabelecidas no ciberespaço demonstram que esse é um campo jurídico em permanente evolução.

Assim, o desenvolvimento do Direito Digital no Brasil demanda não apenas a atualização das normas existentes, mas também o fortalecimento das instituições responsáveis por sua aplicação e a construção de interpretações jurídicas capazes de acompanhar a dinâmica da sociedade digital. Somente a partir desse processo contínuo de adaptação será possível garantir respostas jurídicas mais eficazes diante dos desafios impostos pelas novas formas de criminalidade que emergem no ambiente tecnológico contemporâneo.

Portanto, é possível perceber que o Direito Digital se consolida como um campo jurídico cada vez mais relevante na sociedade contemporânea, exigindo do ordenamento jurídico constante capacidade de adaptação frente às transformações tecnológicas. Mais do que acompanhar a evolução das ferramentas digitais, o desafio do Direito consiste em assegurar que a inovação tecnológica ocorra em consonância com a proteção dos direitos fundamentais, a segurança jurídica e a preservação das garantias individuais. Nesse sentido, o aprimoramento contínuo das normas, das instituições e das interpretações jurídicas mostra-se essencial para que o sistema jurídico brasileiro seja capaz de responder, de forma cada vez mais eficaz, às complexidades e às novas formas de criminalidade que emergem no ambiente digital.

REFERÊNCIAS

BIBLIOTECA DA UNIVERSIDADE PAULISTA - UNIP. **Guia de normalização para apresentação de trabalhos acadêmicos da Universidade Paulista: ABNT**. São Paulo: UNIP, 2025. Disponível em https://unip.br/servicos/biblioteca/guia.aspx. Acesso em: 30. mar. 2026.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 05 abr. 2025.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 07 abr. 2025.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 16 abr. 2025.

PINHEIRO, Patrícia Peck. **Direito Digital**. 7. ed. São Paulo: Saraiva, 2021.
COELHO, Rafael Paulo. **A sociedade digital**. Jusbrasil. Disponível em: https://www.jusbrasil.com.br/artigos/direito-digital/1961307356. Acesso em: 07 abr. 2025.

BRASIL. Ministério das Comunicações. **Portaria Interministerial nº 147, de 31 de maio de 1995**. Disponível em: https://www.cgi.br/portarias/numero/147/. Acesso em: 14 mar. 2026.

SANTOS, Gualtiele Keiber Falcão dos; NASCIMENTO, Emanoel Lourenço do. **Aplicação penal dos cibercrimes contra dignidade sexual**. Revista FT, 2022. Disponível em: https://revistaft.com.br/aplicacao-penal-dos-cibercrimes-contra-dignidade-sexual/. Acesso em: 12 mar. 2025.

SYDOW, Spencer Toth. **Curso de direito penal informático**. 2. ed. rev. e atual. Salvador: JusPodivm, 2021.

MIRANDA, Júlia; MARTINEZ, Diego. **Decisão do TJ/SP inaugura aplicação da LGPD**. Migalhas. Disponível em: https://www.migalhas.com.br/depeso/334657/decisao-do-tj-sp-inaugura-aplicacao-da-lgpd. Acesso em: 20 maio 2025.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 04 jun. 2025.

BRASIL. **Lei nº 9.296, de 24 de julho de 1996**. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Acesso em: 04 jun. 2025.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078.htm. Acesso em: 22 maio 2025.

BRASIL. **Lei nº 14.155, de 27 de maio de 2021**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm. Acesso em: 12 jun. 2025.

SAFERNET BRASIL. **Delegacias especializadas em crimes cibernéticos no Brasil**. Disponível em: https://new.safernet.org.br/content/delegacias-cibercrimes. Acesso em: 14 mar. 2026.

CONSELHO DA EUROPA. **Convenção sobre o Cibercrime (Convenção de Budapeste)**. Budapeste, 23 de novembro de 2001. Série de Tratados do Conselho da Europa, nº 185. Disponível em: https://www.coe.int. Acesso em: 21 set. 2025.

SILVA, Stephane Kamily de Oliveira; ANDRADE, Felipe de. **A evolução dos crimes cibernéticos e os desafios da legislação brasileira**. Revista FT, 2022. Disponível em: https://revistaft.com.br/a-evolucao-dos-crimes-ciberneticos-e-os-desafios-da-legislacao-brasileira/. Acesso em: 11 jun. 2025.

UNIÃO EUROPEIA. **Regulamento (UE) 2022/2065 do Parlamento Europeu e do Conselho, de 19 de outubro de 2022**. Disponível em: https://eur-lex.europa.eu. Acesso em: 10 jan. 2026.

BARRETO, Alesandro Gonçalves; BRASIL, Beatriz Silveira. **Manual de Investigação Cibernética: à luz do Marco Civil da Internet**. Rio de Janeiro: Brasport, 2016.

CNN BRASIL. **País tem 700 milhões de ataques virtuais em um ano, diz relatório**. Disponível em: https://www.cnnbrasil.com.br/economia/negocios/pais-tem-700-milhoes-de-ataques-virtuais-em-um-ano-diz-relatorio/. Acesso em: 19 nov. 2025.

JOTA. **UE é pioneira na regulamentação de sistemas de inteligência artificial**. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/regula-euro/ue-e-pioneira-na-regulamentacao-de-sistemas-de-inteligencia-artificial. Acesso em: 11 jan. 2026.

BRASIL. **Decreto nº 12.573, de 4 de agosto de 2025**. Aprova a Estratégia Nacional de Cibersegurança (E-Ciber). Brasília, DF: Presidência da República, 2025. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/decreto/D12573.htm. Acesso em: 21 fev. 2026.

BRASIL. **Decreto nº 10.748, de 14 de julho de 2021**. Institui a Rede Federal de Gestão de Incidentes Cibernéticos. Brasília, DF: Presidência da República, 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/decreto/d10748.htm. Acesso em: 02 dez. 2025.

BRASIL. **Lei nº 14.460, de 25 de outubro de 2022**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/lei/L14460.htm. Acesso em: 21 nov. 2025.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016**. Disponível em: https://eur-lex.europa.eu. Acesso em: 11 jan. 2026.

BRASIL. Superior Tribunal de Justiça. **Agravo Regimental no Recurso em Habeas Corpus nº 143.169/RJ**. Relator: Jesuíno Rissato (Desembargador convocado). Relator para acórdão: Ribeiro Dantas. Brasília, DF, julgamento em 07 fev. 2023. Diário da Justiça eletrônico, 02 mar. 2023. Disponível em: https://processo.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202100573956&dt_publicacao=02/03/2023. Acesso em: 03 fev. 2026.

BRASIL. Supremo Tribunal Federal. **Arguição de Descumprimento de Preceito Fundamental nº 403**. Relator: Edson Fachin. Brasília, DF, 2016. Disponível em: https://www.stf.jus.br/arquivo/cms/bibliotecaConsultaProdutoBibliotecaPastaFachin/anexo/ADPF403voto.pdf. Acesso em: 09 fev. 2026.

BRASIL. Supremo Tribunal Federal. **Habeas Corpus nº 204.808/SP**. Relator: Alexandre de Moraes. Brasília, DF, 2021. Disponível em: https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/hc204808.pdf. Acesso em: 02 mar. 2026.

BRASIL. Supremo Tribunal Federal. **Inquérito nº 4.781/DF**. Relator: Alexandre de Moraes. Brasília, DF, 2019. Disponível em: https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/mandado27maio.pdf. Acesso em: 04 mar. 2026.

BIBLIOGRAFIA

ADVBOX. **4 casos de inteligência artificial no direito e seus impactos**. Disponível em: https://advbox.com.br/blog/4-casos-de-inteligencia-artificial-no-direito-e-seus-impactos/. Acesso em: 10 mar. 2025.

BRASIL. Autoridade Nacional de Proteção de Dados. **Pesquisa sobre a percepção dos brasileiros sobre proteção de dados e privacidade.** Brasília, DF: ANPD, 2023.

BRASIL. Ministério da Justiça e Segurança Pública. **Estatísticas da Diretoria de Combate a Crimes Cibernéticos (DCIBER)**. Brasília, DF: Polícia Federal, 2024.

CORRADI; MERLINI. **Os desafios do Direito Digital.** Disponível em https://corradiemerlini.com.br/os-desafios-do-direito-digital/. Acesso em: 24 jul. 2025.

ENIAC**. Direito Digital: desafios legais em um ambiente cada vez mais online.** Disponível em: https://www.eniac.edu.br/blog/direito-digital-desafios-legais-em-um-ambiente-cada-vez-mais-online. Acesso em: 10 out. 2025.

ESTADOS UNIDOS. **California Consumer Privacy Act of 2018 (CCPA).** Disponível em: https://ca.gov. Acesso em: 01 maio 2025.

JURISHAND. **A influência da LGPD no Direito Digital.** Disponível em: https://blog.jurishand.com/iinfluencia-da-lgp-direito-digital/. Acesso em: 24 nov. 2025.

LEGALE. **Direito Digital e IA: impactos e desafios jurídicos**. Disponível em: https://legale.com.br/blog/direito-digital-e-ia-impactos-e-desafios-juridicos/. Acesso em: 24 nov. 2025.

MIGALHAS. **Aspectos introdutórios ao Direito Digital.** Disponível em: https://www.migalhas.com.br/depeso/359115/aspectos-introdutorios-ao-direito-digital. Acesso em: 05 out. 2025.

MODELO INICIAL**. Crimes Digitais: o que são e como se prevenir**. Disponível em: https://modeloinicial.com.br/artigos/crimes-digitais. Acesso em: 12 mar. 2026.

OAB NITERÓI. **Cartilha de Direito Digital.** Disponível em: https://oabniteroi.org/wp-content/uploads/2021/10/Cartilha-Direito-Digital-Pronta.pdf. Acesso em: 05 maio 2025.

PROJURIS. **Direito Digital: entenda o que é, sua importância e principais leis.** Disponível em: https://www.projuris.com.br/blog/direito-digital/. Acesso em: 07 abr. 2025.

REVISTA FT. **A evolução do Direito Digital e suas implicações legais**. Disponível em: https://revistaft.com.br/a-evolucao-do-direito-digital-e-suas-implicacoes-legais/ Acesso em: 11 jun. 2025.

SENADO FEDERAL. **Crimes digitais sobem 45% e Senado tem propostas para frear sequestro de dados.** Disponível em: https://www12.senado.leg.br/radio/1/noticia/2025/01/16/crimes-digitais-sobem-45-e-senado-tem-propostas-para-frear-sequestro-de-dados. Acesso em: 10 dez. 2025.

SILVA, Kevin Rick Matias**. A evolução do Direito Digital e seus reflexos no ordenamento jurídico brasileiro.** Disponível em: https://repositorio.pucgoias.edu.br/jspui/bitstream/123456789/1954/1/KEVIN%20RICK%20MATIAS%20SILVA%20-%20tcc.pdf. Acesso em: 15 dez 2025.