



CENTRO DE ESTUDOS SUPERIORES DE ITAITUBA - LTDA
FACULDADE DE ITAITUBA – FAI
CURSO DE BACHARELADO EM DIREITO

WARLLYSON SERRÃO DE SOUSA

**CRIMES DIGITAIS E A DIFICULDADE DE APLICAÇÃO DO DIREITO
PENAL TRADICIONAL: uma revisão de literatura**

Itaituba - PA

2026

WARLLYSON SERRÃO DE SOUSA

CRIMES DIGITAIS E A DIFICULDADE DE APLICAÇÃO DO DIREITO PENAL TRADICIONAL

Trabalho de Conclusão de Curso apresentado à
Faculdade de Itaituba para obtenção de título de
Bacharel em Direito.

Orientador: Prof. Esp. Arleison Glauber Pinheiro
Sousa.

Itaituba - PA

2026

SOUSA, Warllyson Serrão de.

CRIMES DIGITAIS E A DIFICULDADE DE APLICAÇÃO DO DIREITO PENAL TRADICIONAL. Warllyson Serrão de Sousa. Itaituba: FAI, 2026.

66 Fls: il.

Orientador: Prof. Esp. Arleison Glauber Pinheiro Sousa.

Trabalho de Conclusão de Curso (TCC) Graduação em Direito- Faculdade de Itaituba- FAI, 2026.

1. Crimes digitais. 2. Direito penal. I. SOUSA, Arleison Glauber Pinheiro. II. Faculdade de Itaituba, Itaituba, BR-PA, 2026.

WARLLYSON SERRÃO DE SOUSA

CRIMES DIGITAIS E A DIFICULDADE DE APLICAÇÃO DO DIREITO PENAL TRADICIONAL

Trabalho de Conclusão de Curso apresentado à
Faculdade de Itaituba para obtenção de título de
Bacharel em Direito.

Orientador: Prof. Esp. Arleison Glauber Pinheiro
Sousa.

BANCA EXAMINADORA

Avaliador (a) 1: _____ Nota: _____

Avaliador (a) 2: _____ Nota: _____

Resultado: _____ Média: _____

Itaituba: ____ de abril de 2026.

*Dedico essa monografia a Deus e a
minha família, que me deram todo o apoio
para chegar até aqui.*

AGRADECIMENTOS

Primeiramente, agradeço a **Deus** por me conceder força e sabedoria durante esta caminhada.

Ao meu orientador, Prof. **Glauber**, pela dedicação, pela paciência e pelas orientações precisas, que foram fundamentais para a conclusão deste trabalho.

À Faculdade de Itaituba (FAI), por proporcionar a estrutura e o conhecimento necessários à minha formação.

Aos professores do curso de Direito, que compartilharam seus conhecimentos e experiências ao longo da minha trajetória acadêmica.

Aos meus familiares e amigos, pelo apoio incondicional em todos os momentos.

E, por fim, expresso minha gratidão àqueles que, mesmo não estando mais presentes fisicamente, foram e continuam sendo fonte de inspiração, força e motivação ao longo desta trajetória. Suas memórias permanecem vivas em meu coração e fazem parte desta conquista.

RESUMO

O presente trabalho analisa as dificuldades de aplicação do direito penal tradicional aos crimes digitais, considerando o contexto da sociedade da informação e da crescente virtualização das relações sociais e jurídicas. Parte-se do seguinte problema de pesquisa: em que medida um sistema penal estruturado para condutas materiais, territorialmente delimitadas e de autoria identificável consegue responder adequadamente às infrações praticadas por meio de sistemas informáticos ou contra eles. O objetivo geral consiste em analisar os limites do modelo penal clássico diante da criminalidade digital. Como objetivos específicos, busca-se contextualizar esse fenômeno no âmbito da sociedade da informação, conceituar e classificar os crimes digitais, examinar os princípios e a estrutura do direito penal tradicional, bem como identificar os principais entraves à sua aplicação, com destaque para as questões de tipicidade, territorialidade, autoria, materialidade e evolução legislativa brasileira. Justifica-se a pesquisa pela relevância jurídica e social do tema, tendo em vista o crescimento dos crimes praticados em ambiente virtual e os desafios que essas condutas impõem à persecução penal e à tutela de direitos fundamentais. Metodologicamente, trata-se de pesquisa básica, de abordagem qualitativa, desenvolvida por meio de revisão bibliográfica e documental, com enfoque jurídico-dogmático e método dedutivo. Os resultados indicam que, embora já existam avanços doutrinários e legislativos no tratamento da matéria, persistem limitações importantes relacionadas à inadequação de tipos penais concebidos para condutas físicas, à crise

da territorialidade no ciberespaço, às dificuldades de comprovação da autoria e da materialidade e ao descompasso entre a rapidez da inovação tecnológica e a lentidão legislativa. Conclui-se que o direito penal tradicional, apesar de ainda exercer papel relevante, não se mostra plenamente suficiente para enfrentar, de forma integral e garantista, a complexidade da criminalidade digital, o que evidencia a necessidade de contínua reflexão dogmática e de aperfeiçoamento legislativo.

Palavras-chave: Crimes digitais. Direito penal. Sociedade da informação. Tipicidade penal. Evolução legislativa.

ABSTRACT

This paper analyzes the difficulties in applying traditional criminal law to digital crimes, considering the context of the information society and the increasing virtualization of social and legal relations. It starts from the following research problem: to what extent can a criminal justice system structured for materially defined, territorially delimited conduct with identifiable authorship adequately respond to offenses committed through or against computer systems? The general objective is to analyze the limits of the classical criminal model in the face of digital crime. Specific objectives include contextualizing this phenomenon within the information society, conceptualizing and classifying digital crimes, examining the principles and structure of traditional criminal law, and identifying the main obstacles to its application, with emphasis on issues of typicality, territoriality, authorship, materiality, and the evolution of Brazilian legislation. The research is justified by the legal and social relevance of the topic, given the growth of crimes committed in virtual environments and the challenges that these behaviors pose to criminal prosecution and the protection of fundamental rights. Methodologically, this is basic research, with a qualitative approach, developed through bibliographic and documentary review, with a legal-dogmatic focus and deductive method. The results indicate that, although there are already doctrinal and legislative advances in the treatment of the subject, important limitations persist related to the inadequacy of criminal types conceived for physical conduct, the crisis of territoriality in cyberspace, the difficulties in proving authorship and materiality, and the

mismatch between the speed of technological innovation and the slow pace of legislation. It is concluded that traditional criminal law, despite still playing a relevant role, is not fully sufficient to address, in a comprehensive and rights-based manner, the complexity of digital crime, which highlights the need for continuous dogmatic reflection and legislative improvement.

Keywords: Digital crimes. Criminal law. Information society. Criminal typicity. Legislative evolution.

LISTA DE QUADRO

Quadro 1 - Comparativo de estudos analisando os crimes digitais e a dificuldade de aplicação do direito penal tradicional.	38
---	----

SUMÁRIO

1 INTRODUÇÃO	9
2 FUNDAMENTAÇÃO TEÓRICA	11
2.1 SOCIEDADE DA INFORMAÇÃO E TRANSFORMAÇÃO DIGITAL	11
2.2 EVOLUÇÃO TECNOLÓGICA E A SOCIEDADE EM REDE	12
2.3 A INTERNET COMO NOVO ESPAÇO DE INTERAÇÃO SOCIAL	13
2.4 VIRTUALIZAÇÃO DAS RELAÇÕES HUMANAS E JURÍDICAS	14
2.5 IMPACTOS DA TECNOLOGIA NO COMPORTAMENTO SOCIAL E NA CRIMINALIDADE	15
2.6 CONCEITO E CLASSIFICAÇÃO DOS CRIMES DIGITAIS	16
2.7 DIREITO PENAL TRADICIONAL: PRINCÍPIOS E ESTRUTURA CLÁSSICA	22
2.8 A DIFICULDADE DE APLICAÇÃO DO DIREITO PENAL TRADICIONAL AOS CRIMES DIGITAIS	26
2.9 EVOLUÇÃO LEGISLATIVA BRASILEIRA NO COMBATE AOS CRIMES DIGITAIS	30
3 METODOLOGIA	34
3.1 TIPO DE PESQUISA	34
3.2 MÉTODOS DE PESQUISA	35
3.3 COLETA DE DADOS	35
3.4 TÉCNICAS DE ANÁLISE DOS DADOS	36
3.5 CRITÉRIOS DE INCLUSÃO E EXCLUSÃO	36
4 RESULTADOS E DISCUSSÃO	38
4.1 SOCIEDADE DA INFORMAÇÃO, VIRTUALIZAÇÃO DAS RELAÇÕES SOCIAIS E EXPANSÃO DOS CRIMES DIGITAIS	41
4.2 DESAFIOS DO DIREITO PENAL TRADICIONAL FRENTE AOS CRIMES DIGITAIS: TIPICIDADE, PROVA, AUTORIA, TERRITORIALIDADE E INSUFICIÊNCIA LEGISLATIVA	46
5 CONCLUSÃO	53
REFERÊNCIAS	55

1 INTRODUÇÃO

O avanço das tecnologias da informação e da comunicação tem provocado mudanças profundas nas relações sociais, econômicas e institucionais. A sociedade contemporânea passou a ser marcada pela centralidade da informação e pela intensa digitalização das interações humanas.

A ampliação do acesso à internet e o uso massivo de dispositivos tecnológicos modificaram as formas de comunicação, consumo, trabalho e exercício de direitos, ao mesmo tempo em que criaram um ambiente favorável ao surgimento de novas modalidades de condutas ilícitas. Esse contexto corresponde à denominada Sociedade da Informação, na qual a produção, o armazenamento e a circulação de dados assumem papel estratégico na organização da vida social (RODRIGUES, 2022).

Nesse cenário, os crimes digitais, praticados total ou parcialmente por meio de sistemas informáticos e ambientes virtuais, apresentam peculiaridades como a imaterialidade das condutas, a dispersão geográfica dos agentes e a dificuldade de identificação da autoria e da materialidade.

Tais características evidenciam limites do direito penal tradicional, cuja estrutura foi concebida para regular condutas ocorridas em contextos físicos, territorialmente delimitados e passíveis de identificação direta dos sujeitos envolvidos. A adaptação desse modelo clássico às novas dinâmicas do ciberespaço mostra-se complexa e, em muitos casos, insuficiente para assegurar uma tutela penal eficaz (MARTINS, 2024).

Diante desse quadro, coloca-se o seguinte problema de pesquisa: em que medida o direito penal tradicional é capaz de responder de forma adequada às condutas ilícitas praticadas no ambiente digital? A incompatibilidade entre os pressupostos clássicos do sistema penal e as particularidades da criminalidade digital suscita questionamentos acerca da efetividade das normas existentes, da adequação dos tipos penais tradicionais e da observância dos princípios fundamentais que limitam o poder punitivo estatal, como a legalidade, a tipicidade e a culpabilidade.

A relevância do estudo se justifica tanto no plano jurídico quanto no social. No âmbito jurídico, a pesquisa auxilia na compreensão das dificuldades enfrentadas pelo ordenamento penal diante das transformações tecnológicas, evidenciando lacunas normativas e desafios interpretativos que impactam a persecução penal dos crimes

digitais. No plano social, o tema mostra-se pertinente diante do aumento significativo dessas práticas ilícitas e dos reflexos que produzem sobre direitos fundamentais, como a privacidade, a segurança da informação e a dignidade da pessoa humana.

Nesse contexto, o objetivo geral deste trabalho consiste em analisar as dificuldades de aplicação do direito penal tradicional aos crimes digitais, considerando as características do ambiente virtual e as limitações estruturais do modelo penal clássico.

Como objetivos específicos, busca-se identificar de que maneira a sociedade da informação e a virtualização das relações sociais contribuíram para a expansão dos crimes digitais, analisar os fundamentos do direito penal tradicional aplicáveis ao ambiente digital, verificar os principais entraves à repressão penal dessas condutas, especialmente quanto à tipicidade, territorialidade, autoria, materialidade e prova digital, e avaliar se a evolução legislativa tem sido suficiente para enfrentar tais dificuldades.

Para alcançar os objetivos propostos, adotou-se como metodologia, a pesquisa bibliográfica, com abordagem qualitativa, pesquisa exploratória e descritiva baseada na análise de obras doutrinárias, artigos científicos, legislação nacional e documentos oficiais pertinentes ao tema.

Quanto à estrutura, o trabalho organiza-se em cinco seções. A primeira corresponde à introdução, na qual são expostos o tema central, os objetivos propostos e a problemática que orientou a pesquisa. Na segunda seção, desenvolve-se a fundamentação teórica, abordando a sociedade da informação e transformação digital, além de discutir impactos da tecnologia no comportamento social e na criminalidade e a evolução legislativa brasileira no combate aos crimes digitais.

A terceira seção apresenta a metodologia adotada, descrevendo os métodos e instrumentos que compuseram o estudo. Na quarta seção, apresenta e discute os resultados obtidos. Por fim, a quinta seção destina-se às conclusões, estabelecendo um confronto entre os objetivos inicialmente definidos e os dados levantados ao longo da pesquisa.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 SOCIEDADE DA INFORMAÇÃO E TRANSFORMAÇÃO DIGITAL

A expressão “Sociedade da Informação” refere-se a um estágio de desenvolvimento social no qual a informação assume papel central na organização das relações econômicas, políticas e culturais. Nesse modelo social, a produção, o armazenamento e a circulação de informações tornam-se elementos estratégicos, capazes de influenciar decisões individuais e coletivas. Tal configuração é resultado direto do avanço das tecnologias da informação e da comunicação, que ampliaram significativamente a capacidade de processamento e difusão de dados em escala global (SOARES, 2016).

A expressão "sociedade da informação" passou a ser utilizada, nos últimos anos desse século, como substituto para o conceito complexo de "sociedade pós-industrial" e como forma de transmitir o conteúdo específico do "novo paradigma técnico-econômico (WERTHEIN, 2000, p. 71).

O desenvolvimento tecnológico promoveu uma reestruturação dos meios de comunicação e das formas de interação social. A digitalização da informação permitiu que conteúdos fossem transmitidos de maneira instantânea, superando limitações geográficas e temporais que, historicamente, condicionavam as relações humanas. Como consequência, a informação deixou de ocupar posição acessória e passou a constituir um dos principais pilares da vida social contemporânea (RODRIGUES, 2022).

Nesse contexto, observa-se uma intensificação da dependência social em relação aos sistemas tecnológicos. Atividades cotidianas, como comunicação interpessoal, relações de consumo, acesso a serviços públicos e exercício de direitos fundamentais, passaram a ocorrer, em grande medida, por meio de plataformas digitais. A centralidade da informação redefine, portanto, a forma como os indivíduos se relaciona entre si e com as instituições (OLIVEIRA, 2023).

Para Vilaça e Araújo (2016), a transformação digital não se limita à introdução de novas ferramentas tecnológicas, mas implica uma mudança estrutural na dinâmica social, a incorporação massiva de tecnologias digitais alterou padrões de comportamento, formas de organização social e mecanismos de controle. Essa

realidade impacta diretamente o campo jurídico, na medida em que os modelos normativos tradicionais foram concebidos para regular relações estabelecidas em contextos predominantemente físicos.

O Direito, enquanto instrumento de regulação social, passa a enfrentar desafios decorrentes da complexidade do ambiente informacional. A velocidade com que as informações são produzidas e disseminadas contrasta com a rigidez e a lentidão inerentes ao processo legislativo (ÂNGELO, 2025).

Tal descompasso evidencia dificuldades na adaptação das normas jurídicas às novas práticas sociais emergentes no meio digital. No âmbito do direito penal, essas transformações assumem relevância particular. A Sociedade da Informação cria condições favoráveis ao surgimento de novas formas de criminalidade, bem como à adaptação de delitos tradicionais ao ambiente digital. A utilização de tecnologias para a prática de condutas ilícitas desafia categorias clássicas do direito penal, como territorialidade, autoria e materialidade do crime (MARTINS, 2024).

Como aponta Veloso Filho (2025), torna-se necessária uma reflexão crítica sobre a capacidade do ordenamento jurídico penal de responder às demandas impostas pela transformação digital, a análise da sociedade da informação revela que o fenômeno tecnológico não apenas modifica a forma como os crimes são praticados, mas também expõe limitações estruturais do direito penal tradicional, justificando a investigação proposta neste trabalho.

2.2 EVOLUÇÃO TECNOLÓGICA E A SOCIEDADE EM REDE

De acordo com Silva Monteiro e Façanha (2025), a evolução tecnológica constitui elemento fundamental para a consolidação da denominada sociedade em rede. Esse modelo social caracteriza-se pela interconexão permanente entre indivíduos, grupos e instituições por meio de sistemas digitais de comunicação. A expansão das redes informacionais possibilitou a criação de estruturas descentralizadas, nas quais a circulação de dados ocorre de forma contínua e em tempo real.

A internet desempenha papel central nesse processo, ao permitir a integração de diferentes atores sociais em um mesmo ambiente virtual. A comunicação mediada por redes digitais altera significativamente as formas tradicionais de interação, substituindo modelos hierarquizados por estruturas mais flexíveis e dinâmicas. Essa

reorganização social amplia as possibilidades de participação, ao mesmo tempo em que redefine relações de poder e controle (GUINEZI, 2020).

A sociedade em rede também modifica a forma como as atividades econômicas, políticas e culturais são desenvolvidas. Processos produtivos passaram a depender de fluxos informacionais, enquanto decisões institucionais e práticas sociais são influenciadas pela rapidez e pelo alcance das redes digitais. Nesse contexto, a informação assume valor estratégico, reforçando sua centralidade na organização da vida social (NUNES, 2016).

Sob a perspectiva jurídica, a sociedade em rede impõe desafios relevantes ao ordenamento normativo. As normas tradicionais foram elaboradas a partir de uma concepção territorial e material das relações sociais, o que se mostra insuficiente diante de um ambiente marcado pela fluidez e pela ausência de fronteiras definidas. A atuação em rede dificulta a identificação precisa de locais, agentes e circunstâncias dos atos praticados (SANTOS; OLIVEIRA, 2025).

No campo do direito penal, essas dificuldades tornam-se ainda mais evidentes. A estrutura em rede favorece a prática de condutas ilícitas que se beneficiam do anonimato e da dispersão geográfica dos agentes. A descentralização das redes digitais compromete a aplicação de critérios clássicos de competência e responsabilidade penal, exigindo interpretações mais complexas das normas existentes (MELLO, 2022).

2.3 A INTERNET COMO NOVO ESPAÇO DE INTERAÇÃO SOCIAL

A internet consolidou-se como um novo espaço de interação social, no qual se desenvolvem relações pessoais, profissionais, econômicas e institucionais. A ampliação do acesso às redes digitais permitiu que indivíduos e grupos passassem a interagir de forma contínua em ambientes virtuais, integrando o ciberespaço à dinâmica cotidiana da sociedade contemporânea (NUNES, 2025).

Segundo Lima (2022), as interações mediadas pela internet apresentam características próprias, como a instantaneidade, a ampliação do alcance comunicacional e a possibilidade de anonimato, esses elementos transformaram os padrões tradicionais de sociabilidade, permitindo que relações antes condicionadas à presença física ocorressem de maneira remota e simultânea. A internet, nesse

sentido, não se limita a um instrumento de comunicação, mas configura-se como um ambiente social autônomo.

Esse novo espaço de interação favoreceu a expansão de práticas sociais diversas, incluindo o exercício de atividades profissionais, a circulação de informações e a formação de vínculos interpessoais. Ao mesmo tempo, a virtualização dessas relações reduziu barreiras geográficas e temporais, contribuindo para a intensificação dos fluxos informacionais e para a redefinição das fronteiras entre o público e o privado (BRASILEIRO, 2017).

Para Carvalho (2024), do ponto de vista jurídico, a internet apresenta desafios específicos, uma vez que as normas tradicionais foram elaboradas a partir de uma concepção de espaço físico claramente delimitado. No ambiente digital, as interações ocorrem de forma difusa, dificultando a identificação precisa dos sujeitos envolvidos e do local de ocorrência dos fatos. Essa realidade impacta diretamente a aplicação do Direito, especialmente no campo penal.

Martins (2024) aponta que, no âmbito do direito penal, a internet como espaço de interação social amplia as possibilidades de prática de condutas ilícitas. A facilidade de comunicação e a rapidez na disseminação de informações potencializam a ocorrência de delitos, ao mesmo tempo em que dificultam a atuação dos órgãos de persecução penal.

Tais circunstâncias evidenciam a necessidade de uma análise crítica acerca da adequação dos instrumentos jurídicos tradicionais frente às novas formas de interação social mediadas pela tecnologia.

2.4 VIRTUALIZAÇÃO DAS RELAÇÕES HUMANAS E JURÍDICAS

A virtualização das relações humanas consiste no deslocamento progressivo das interações sociais para o ambiente digital. Esse fenômeno resulta da incorporação das tecnologias da informação e da comunicação ao cotidiano, promovendo a mediação tecnológica de práticas antes realizadas exclusivamente no espaço físico. Como consequência, as relações interpessoais passaram a ocorrer, em larga medida, por meio de plataformas digitais (JURKEVICZ, 2017).

Esse processo não se restringe às relações de caráter pessoal, alcançando também as relações jurídicas. A utilização de meios eletrônicos para a formalização de contratos, a comunicação entre as partes e a prática de atos jurídicos tornou-se

comum, evidenciando a ampliação do espaço virtual como ambiente legítimo de produção de efeitos jurídicos. A virtualização altera, assim, a forma de manifestação da vontade e de exercício de direitos e deveres (PEREIRA, 2022).

Segundo Albano (2023), no campo jurídico, a virtualização das relações impõe desafios relevantes à segurança jurídica, a circulação de documentos digitais, a utilização de assinaturas eletrônicas e o armazenamento de informações em meios virtuais exigem mecanismos eficazes de proteção e autenticidade. A ausência ou fragilidade desses mecanismos pode comprometer a confiabilidade das relações estabelecidas no ambiente digital.

No âmbito penal, a virtualização favorece a prática de condutas ilícitas que se aproveitam da imaterialidade do meio digital. A possibilidade de ocultação da identidade dos agentes e a dificuldade de rastreamento das ações realizadas no ambiente virtual dificultam a identificação da autoria e a produção de provas. Tais fatores contribuem para o aumento da complexidade na investigação e repressão dos crimes digitais (XAVIER, 2025).

Dessa forma, a virtualização das relações humanas e jurídicas evidencia a necessidade de adequação do ordenamento jurídico às novas dinâmicas sociais. A análise desse fenômeno revela limitações do modelo jurídico tradicional, especialmente no que se refere à aplicação das normas penais, reforçando a importância de uma reflexão crítica sobre os instrumentos normativos existentes frente à realidade digital (LUSTOSA, 2025).

2.5 IMPACTOS DA TECNOLOGIA NO COMPORTAMENTO SOCIAL E NA CRIMINALIDADE

O avanço das tecnologias da informação e da comunicação provocou mudanças significativas no comportamento social contemporâneo. A ampliação do acesso à internet e a disseminação de dispositivos digitais alteraram hábitos, formas de comunicação e padrões de interação entre os indivíduos. A tecnologia passou a integrar o cotidiano social, influenciando a maneira como as pessoas se informam, se relacionam e exercem atividades diversas.

Essas transformações refletiram-se na intensificação das interações mediadas por ambientes digitais. A exposição constante em redes sociais, a rapidez na circulação de informações e a redução das barreiras espaciais modificaram a

percepção de privacidade e de responsabilidade social. Tais mudanças contribuíram para a redefinição de limites entre o espaço público e o privado, gerando novos desafios para a convivência social (VILAÇA; ARAÚJO, 2016).

De acordo com Martins (2024), no âmbito da criminalidade, os impactos da tecnologia são igualmente relevantes. O ambiente digital ampliou as possibilidades de prática de condutas ilícitas, seja pela criação de novos tipos de crimes, seja pela adaptação de delitos tradicionais ao meio virtual. A utilização de recursos tecnológicos favorece a execução de crimes de forma mais rápida e com menor risco de identificação imediata dos agentes.

A criminalidade digital apresenta características próprias, como a imaterialidade das condutas, a dispersão geográfica dos envolvidos e a complexidade técnica dos meios utilizados. Esses elementos dificultam a atuação dos órgãos de investigação e a aplicação dos mecanismos tradicionais de repressão penal. A produção e a valoração da prova, bem como a identificação da autoria, tornam-se mais complexas no contexto digital (MARTINS, 2023).

Diante desse cenário, evidencia-se que o comportamento social influenciado pela tecnologia está diretamente relacionado à transformação das práticas criminosas. O direito penal, estruturado a partir de pressupostos clássicos, enfrenta limitações para responder de forma eficaz às novas formas de criminalidade. A análise dos impactos da tecnologia no comportamento social e na criminalidade revela, portanto, a necessidade de adaptação do ordenamento penal às exigências da sociedade da informação, tema que será aprofundado nos capítulos seguintes (GOMES; CRUZ, 2019).

2.6 CONCEITO E CLASSIFICAÇÃO DOS CRIMES DIGITAIS

Segundo Maia (2017), o avanço das tecnologias da informação e da comunicação contribuiu para o surgimento de novas formas de criminalidade, praticadas total ou parcialmente por meio de sistemas informáticos. A ampliação do uso da internet e de dispositivos digitais criou um ambiente propício à ocorrência de condutas ilícitas que desafiam os modelos tradicionais de repressão penal, exigindo uma análise específica no âmbito do direito penal.

Os crimes digitais apresentam características próprias, relacionadas à imaterialidade do meio, à facilidade de disseminação das condutas e à complexidade

técnica envolvida em sua prática. Essas particularidades dificultam a aplicação dos conceitos penais clássicos, especialmente no que se refere à definição dos tipos penais, à identificação da autoria e à delimitação do local do crime (TRIVINO, 2024).

Torna-se necessário delimitar o conceito de crimes digitais, bem como estabelecer critérios de classificação que permitam compreender suas diferentes modalidades. Os crimes digitais, também denominados crimes cibernéticos, consistem em condutas ilícitas praticadas por meio de sistemas informáticos ou contra esses sistemas, utilizando-se de tecnologias da informação e da comunicação como instrumento, meio ou finalidade da ação criminosa. Trata-se de fenômeno diretamente relacionado ao desenvolvimento da Sociedade da Informação e à ampliação do uso da internet no cotidiano social (SILVA, 2022).

A doutrina não apresenta um conceito único e definitivo para os crimes digitais, em razão da constante evolução tecnológica e da diversidade de condutas abrangidas por essa categoria. De modo geral, compreendem-se como crimes digitais aquelas infrações penais que envolvem o uso de dispositivos eletrônicos, redes de computadores ou ambientes virtuais para a prática de atos ilícitos, independentemente de estarem ou não expressamente tipificados na legislação penal específica (OLIVEIRA; ÁVILA, 2024).

Nesse sentido, os crimes digitais podem se manifestar tanto como novas formas de criminalidade quanto como adaptações de delitos tradicionais ao meio virtual. Condutas como fraude, ameaça, violação de sigilo e estelionato passaram a ser praticadas em ambiente digital, mantendo sua essência típica, mas assumindo novas formas de execução. Paralelamente, surgiram delitos cuja existência depende diretamente da tecnologia, como a invasão de dispositivos informáticos (HENRIQUES; GONÇALVES, 2024).

Segundo Xavier (2025), a utilização do meio digital confere aos crimes cibernéticos características próprias, tais como a imaterialidade da conduta, a possibilidade de anonimato dos agentes e a ampla dispersão geográfica dos envolvidos. Essas particularidades dificultam a identificação da autoria, a delimitação do local do crime e a produção de provas, tornando mais complexa a atuação dos órgãos de persecução penal.

Ainda segundo o autor, do ponto de vista jurídico-penal, o conceito de crimes digitais evidencia a insuficiência do modelo tradicional de tipificação frente às novas dinâmicas sociais. A ausência de fronteiras claras no ambiente virtual e a rápida

mutação das tecnologias impõem desafios à aplicação dos tipos penais clássicos, exigindo interpretações extensivas e, em alguns casos, a criação de normas específicas (XAVIER, 2025).

A compreensão conceitual dos crimes digitais constitui etapa fundamental para a análise de sua classificação e para a discussão acerca das dificuldades de aplicação do direito penal tradicional. A delimitação do conceito permite identificar as particularidades dessa modalidade criminosa e fundamentar a necessidade de adequação do ordenamento jurídico às exigências da realidade digital contemporânea (SOUSA, 2023).

A literatura jurídica e criminológica utiliza diferentes terminologias para se referir às infrações penais relacionadas ao uso de tecnologias da informação e da comunicação. Expressões como crimes informáticos, crimes virtuais e cibercrimes são frequentemente empregadas de forma indistinta, embora apresentem nuances conceituais relevantes. A ausência de uniformidade terminológica decorre, em grande medida, da evolução constante do meio tecnológico e da diversidade de condutas abrangidas por essas denominações (JUSTINIANO, 2024).

A expressão “crimes informáticos” é tradicionalmente utilizada para designar as infrações que têm como objeto direto os sistemas computacionais ou os dados neles armazenados. Nesse sentido, o computador ou o sistema informático constitui o alvo principal da conduta criminosa. Exemplificam-se, nesse grupo, práticas como a invasão de sistemas, a destruição ou alteração de dados e o acesso não autorizado a informações protegidas (SANTOS, 2021).

O termo “crime virtual”, por sua vez, costuma ser empregado para se referir às condutas ilícitas praticadas no ambiente da internet, independentemente de o sistema informático ser o objeto ou apenas o meio da ação criminosa. Essa terminologia enfatiza o espaço virtual como local de ocorrência do delito, abrangendo tanto crimes específicos do meio digital quanto delitos tradicionais executados por meio de plataformas online (BESTETTI, 2023).

Segundo Silva (2019), já a expressão cibercrimes, amplamente difundida na doutrina contemporânea e em documentos internacionais, apresenta caráter mais abrangente, o termo compreende qualquer infração penal relacionada ao ciberespaço, incluindo aquelas em que a tecnologia é utilizada como instrumento, meio ou finalidade da conduta. Os cibercrimes englobam, portanto, tanto os crimes

informáticos quanto os crimes virtuais, funcionando como categoria mais ampla de classificação.

Do ponto de vista jurídico, a multiplicidade terminológica pode gerar dificuldades interpretativas, especialmente na aplicação das normas penais. A falta de precisão conceitual compromete a delimitação do objeto da tutela penal e dificulta a sistematização das condutas ilícitas no ordenamento jurídico. Ainda assim, a doutrina tende a adotar a expressão crimes digitais ou cibercrimes como forma de abranger, de maneira mais ampla, as diversas manifestações da criminalidade no ambiente tecnológico (TENÓRIO, 2022).

Assim Justiniano (2024) destaca que a análise das terminologias correlatas revela a complexidade conceitual que envolve os crimes praticados no meio digital, a compreensão dessas expressões é essencial para a correta classificação das condutas e para a avaliação das dificuldades enfrentadas pelo direito penal tradicional diante da criminalidade contemporânea.

De acordo com Trivino (2024), a classificação dos crimes digitais constitui instrumento relevante para a compreensão das diversas formas de criminalidade associadas ao uso das tecnologias da informação e da comunicação, a sistematização dessas condutas permite identificar as particularidades de cada modalidade, bem como avaliar os desafios específicos que elas impõem ao direito penal tradicional.

A doutrina majoritária adota uma classificação que distingue os crimes digitais em próprios, impróprios e mistos ou híbridos. Tal divisão baseia-se no papel desempenhado pela tecnologia na prática do delito, considerando se o meio digital constitui o objeto da conduta, apenas o instrumento utilizado ou ambos simultaneamente (BROCHADO, 2025).

Segundo Silva (2022), os crimes próprios digitais são aqueles cuja existência depende diretamente da utilização de sistemas informáticos ou do ambiente digital. Nessa modalidade, a tecnologia constitui o próprio objeto da conduta criminosa, sendo indispensável para a configuração do delito. Sem a presença do meio digital, a prática criminosa não poderia ocorrer.

Esses crimes têm como alvo principal os sistemas computacionais, redes de dados ou informações armazenadas em meio eletrônico. A violação recai sobre a integridade, a confidencialidade ou a disponibilidade dos sistemas informáticos, evidenciando a proteção penal do bem jurídico relacionado à segurança da informação (MAIA, 2017).

Tais delitos evidenciam a necessidade de tipos penais específicos, uma vez que não encontram correspondência direta nas figuras tradicionais do direito penal clássico.

Os crimes impróprios digitais correspondem às infrações penais tradicionais que passam a ser praticadas por meio de instrumentos tecnológicos. Nessa categoria, o meio digital não constitui o objeto do delito, mas apenas o instrumento utilizado para sua execução, a essência típica da conduta permanece a mesma, independentemente do ambiente em que é praticada (SOARES, 2019).

Delitos como estelionato, ameaça, injúria, difamação e falsidade documental podem ser cometidos tanto no espaço físico quanto no ambiente virtual. A utilização da internet ou de sistemas informáticos apenas modifica a forma de execução da conduta, sem alterar sua natureza jurídica fundamental (SANTOS *et al.*, 2024).

Como afirma Farias *et al.* (2022), a criação de novos tipos penais, os crimes impróprios digitais apresentam desafios relevantes para a aplicação do direito penal. A identificação da autoria, a produção de provas e a delimitação do local do crime tornam-se mais complexas quando a conduta ocorre no ambiente digital, exigindo adaptações interpretativas e procedimentais.

Segundo Ferreira Filho e Torre (2024), os crimes mistos ou híbridos caracterizam-se pela combinação de elementos dos crimes próprios e impróprios digitais. Nessa modalidade, a tecnologia desempenha papel duplo, atuando simultaneamente como meio e como objeto da conduta criminosa. Trata-se de categoria que evidencia a complexidade crescente da criminalidade no contexto da sociedade da informação.

Ainda segundo o autor, nesses casos, a prática delitiva envolve tanto a utilização de sistemas informáticos quanto a violação de bens jurídicos tradicionais, como o patrimônio, a honra ou a liberdade individual. A conduta criminosa não se limita à ofensa ao sistema digital, mas produz efeitos jurídicos que extrapolam o ambiente virtual (FERREIRA FILHO; TORRE, 2024).

Os crimes híbridos desafiam de forma ainda mais intensa o direito penal tradicional, pois demandam uma interpretação integrada das normas existentes. A sobreposição de bens jurídicos tutelados e a multiplicidade de elementos envolvidos na conduta dificultam a subsunção do fato aos tipos penais clássicos, reforçando a necessidade de atualização e adequação do ordenamento jurídico penal (OLIVEIRA, 2022).

No contexto brasileiro, a criminalidade digital manifesta-se por meio de diversas espécies de delitos que refletem tanto a adaptação de crimes tradicionais ao ambiente virtual quanto o surgimento de condutas ilícitas próprias da era digital. A ampliação do acesso à internet e a utilização massiva de dispositivos tecnológicos favoreceram a disseminação dessas práticas, exigindo respostas normativas específicas por parte do ordenamento jurídico penal (MAIA, 2017).

Entre as principais espécies de crimes digitais no Brasil, destacam-se aqueles relacionados à invasão de dispositivos informáticos. Essas condutas envolvem o acesso não autorizado a sistemas computacionais, com o objetivo de obter, adulterar ou destruir dados. Trata-se de modalidade criminosa que atinge diretamente a segurança da informação e evidencia a necessidade de proteção penal específica aos sistemas digitais (FERNANDES, 2022).

De acordo com Henriques e Gonçalves (2024), as fraudes eletrônicas também ocupam posição relevante no cenário da criminalidade digital brasileira, o estelionato praticado por meio da internet, de aplicativos de mensagens e de plataformas digitais tornou-se recorrente, explorando a confiança das vítimas e a dificuldade de verificação imediata das informações. Embora se trate de crime tradicional, sua prática no ambiente digital potencializa o alcance da conduta e amplia o número de vítimas envolvidas.

Outra espécie significativa refere-se aos crimes contra a honra praticados no meio digital. Ofensas como injúria, difamação e calúnia passaram a ocorrer com frequência em redes sociais e outros espaços virtuais de interação. A rapidez na disseminação das mensagens e o alcance ampliado das publicações intensificam os danos causados às vítimas, ao mesmo tempo em que dificultam a responsabilização dos autores (SOARES, 2020).

Os crimes relacionados à violação de dados pessoais e à privacidade também assumem relevância no contexto brasileiro. A coleta, o compartilhamento e o uso indevido de informações pessoais em ambientes digitais configuram condutas ilícitas que afetam diretamente direitos fundamentais. Essas práticas evidenciam a fragilidade da proteção da intimidade no ambiente virtual e reforçam a necessidade de mecanismos legais eficazes (MAROUF, 2024).

2.7 DIREITO PENAL TRADICIONAL: PRINCÍPIOS E ESTRUTURA CLÁSSICA

O direito penal tradicional constitui o principal instrumento de repressão estatal às condutas consideradas mais gravosas à ordem social. Sua construção teórica e normativa fundamenta-se em princípios consolidados e em uma estrutura dogmática desenvolvida ao longo do tempo, voltada à proteção de bens jurídicos relevantes e à limitação do poder punitivo do Estado (BAPTISTA, 2020).

Historicamente, o modelo penal clássico foi elaborado a partir de pressupostos relacionados à materialidade das condutas, à territorialidade do delito e à identificação direta do agente. Esses elementos orientaram a formulação dos tipos penais e a aplicação das sanções, tendo como referência uma realidade social marcada por interações predominantemente físicas e localizadas (PEREIRA, 2024).

Segundo Garmes (2025), a consolidação dos princípios penais, como a legalidade, a tipicidade e a culpabilidade, desempenha papel fundamental na garantia da segurança jurídica e na proteção dos direitos fundamentais. Tais princípios estruturam a atuação do Estado no exercício do *jus puniendi*, estabelecendo limites claros à intervenção penal e assegurando previsibilidade na aplicação da lei.

Como aponta Eisele (2018), direito penal pode ser compreendido como o ramo do ordenamento jurídico responsável por definir as condutas consideradas crimes e por estabelecer as sanções aplicáveis aos seus autores. Trata-se de instrumento de controle social exercido pelo Estado, cuja atuação incide sobre comportamentos que atentam de forma mais grave contra bens jurídicos fundamentais à convivência social.

A função primordial do direito penal consiste na proteção desses bens jurídicos, tais como a vida, a liberdade, o patrimônio e a dignidade da pessoa humana, a intervenção penal justifica-se apenas quando outros ramos do direito se mostram insuficientes para tutelar tais interesses, razão pela qual o direito penal é orientado pelo caráter de *ultima ratio*. Esse aspecto reforça a necessidade de uma aplicação restritiva e criteriosa das normas penais (SALIM; AZEVEDO, 2019).

Além da função protetiva, o direito penal exerce função preventiva, tanto em sua dimensão geral quanto especial. A prevenção geral busca desestimular a prática de delitos por meio da ameaça de sanção, enquanto a prevenção especial volta-se à ressocialização do infrator e à redução da reincidência. Essas finalidades evidenciam o caráter normativo e pedagógico do sistema penal (MORAES, 2022).

Como aponta Coelho (2020), o direito penal também possui função limitadora do poder punitivo estatal. Ao definir previamente as condutas proibidas e as penas correspondentes, o ordenamento penal estabelece parâmetros objetivos para a atuação do Estado, garantindo segurança jurídica e previsibilidade.

Essa limitação é fundamental para a proteção dos direitos e garantias individuais frente ao exercício do *jus puniendi*. Nesse sentido, o conceito e a finalidade do direito penal estão diretamente relacionados à necessidade de equilíbrio entre a repressão das condutas ilícitas e a preservação das liberdades individuais. A estrutura normativa penal não se destina apenas à punição, mas à manutenção da ordem social dentro de limites juridicamente estabelecidos (TAVARES, 2024).

Contudo, as transformações sociais decorrentes do avanço tecnológico desafiam a efetividade dessas finalidades, o surgimento de novas formas de criminalidade, especialmente no ambiente digital, evidencia a dificuldade do direito penal tradicional em cumprir suas funções protetiva e preventiva de maneira eficaz, o que reforça a importância da análise crítica proposta neste trabalho (XAVIER, 2025).

Os princípios fundamentais do direito penal constituem a base axiológica e normativa desse ramo jurídico, orientando tanto a elaboração das normas penais quanto a sua aplicação concreta. Esses princípios exercem função essencial na limitação do poder punitivo do Estado, assegurando a proteção dos direitos fundamentais e a observância da segurança jurídica (SALIM; AZEVEDO, 2019).

Segundo Santos e Ferreira (2024), o princípio da legalidade constitui um dos pilares fundamentais do direito penal, estabelecendo que não há crime nem pena sem lei anterior que os defina. Tal princípio consagra a exigência de que somente a lei, em sentido formal, pode criar tipos penais e cominar sanções, vedando qualquer forma de incriminação baseada em costumes, analogia ou discricionariedade estatal.

A legalidade penal exerce função essencial de garantia, ao assegurar previsibilidade e segurança jurídica aos indivíduos. A definição prévia e escrita das condutas proibidas permite que os cidadãos conheçam, antecipadamente, os limites de atuação impostos pelo ordenamento jurídico, protegendo-os contra intervenções arbitrárias do Estado no exercício do poder punitivo (VIANA, 2021).

Como aponta Medeiros e Nelson (2016), esse princípio também impõe limites à atividade interpretativa dos órgãos jurisdicionais, a aplicação da norma penal deve respeitar os contornos estabelecidos pelo legislador, sendo vedadas interpretações extensivas ou analógicas que ampliem o alcance do tipo penal em prejuízo do

acusado. Dessa forma, a legalidade atua como mecanismo de contenção do *jus puniendi* e de preservação das liberdades individuais.

No contexto da criminalidade digital, o princípio da legalidade enfrenta desafios significativos. A rápida evolução tecnológica frequentemente antecede a produção legislativa, resultando em lacunas normativas diante de novas condutas ilícitas praticadas no ambiente digital. Essa defasagem dificulta a tipificação penal de determinados comportamentos e evidencia a tensão entre a necessidade de repressão penal e a observância estrita da legalidade (VALENTE, 2018).

Assim, o princípio da legalidade revela-se central para a análise das dificuldades de aplicação do direito penal tradicional aos crimes digitais. A exigência de tipificação prévia limita a atuação estatal frente a condutas emergentes, reforçando a necessidade de reflexão acerca da adequação do modelo penal clássico às transformações impostas pela sociedade da informação.

O princípio da tipicidade decorre diretamente do princípio da legalidade e consiste na exigência de que a conduta praticada se adeque, de forma precisa, à descrição contida no tipo penal. Para que haja crime, é necessário que o fato concreto corresponda exatamente ao modelo abstrato previsto em lei, não sendo admitida a punição de comportamentos que não estejam claramente tipificados (PLENS, 2025).

De acordo com Rocha (2022), a tipicidade é importante na delimitação do âmbito de incidência do direito penal, ao exigir a correspondência estrita entre a conduta e o tipo legal, esse princípio assegura a objetividade da aplicação da norma penal e impede interpretações ampliativas que possam resultar em responsabilização indevida. Trata-se de mecanismo essencial para a preservação da segurança jurídica.

Além de sua dimensão formal, a tipicidade também possui aspecto material, relacionado à efetiva lesão ou ameaça de lesão ao bem jurídico tutelado. Não basta que a conduta se enquadre formalmente na descrição legal; é necessário que ela apresente relevância penal suficiente para justificar a intervenção do Estado. Esse aspecto reforça o caráter seletivo e restritivo do direito penal (RESENDE; MOLINARO, 2019).

No contexto dos crimes digitais, o princípio da tipicidade enfrenta desafios relevantes. Muitas condutas praticadas no ambiente virtual não encontram correspondência direta nos tipos penais tradicionais, elaborados para regular comportamentos ocorridos no espaço físico. Essa incompatibilidade dificulta a

subsunção dos fatos às normas existentes e pode comprometer a efetividade da repressão penal (FLORES, 2025).

Segundo David (2016), o princípio da culpabilidade estabelece que a imposição de pena somente é legítima quando houver possibilidade de reprovação pessoal da conduta praticada pelo agente. A responsabilidade penal exige que o autor do fato tenha agido com dolo ou culpa, além de possuir capacidade de compreender o caráter ilícito da conduta e de determinar-se de acordo com esse entendimento.

Esse princípio afasta a responsabilização penal objetiva, vedando a imposição de sanções sem a análise da vontade e da consciência do agente. A culpabilidade funciona, portanto, como elemento indispensável para a individualização da pena, assegurando que a resposta estatal seja dirigida exclusivamente a quem efetivamente pode ser responsabilizado pelo fato ilícito (CANESTRARO; JANUÁRIO, 2018).

A análise da culpabilidade envolve a verificação de elementos como imputabilidade, potencial consciência da ilicitude e exigibilidade de conduta diversa. Esses aspectos permitem avaliar se o agente poderia agir de maneira distinta daquela praticada, considerando suas condições pessoais e as circunstâncias do caso concreto. Tal avaliação reforça o caráter pessoal e subjetivo da responsabilidade penal (CORTEZ, 2017).

No âmbito dos crimes digitais, a aplicação do princípio da culpabilidade apresenta desafios específicos. A complexidade técnica dos meios utilizados e a possibilidade de utilização de sistemas automatizados ou de terceiros dificultam a identificação da intenção do agente e a atribuição da conduta a um sujeito determinado. Em alguns casos, torna-se difícil comprovar o dolo ou a culpa de forma inequívoca (HAMMERSCHMIDT; DAVID, 2023).

Como destaca Hammerschmidt e David (2023), a estrutura clássica do crime, consagrada pela dogmática penal, compreende o crime como um fato típico, ilícito e culpável. Essa concepção tripartida constitui base fundamental do direito penal tradicional e orienta a análise da responsabilidade penal, permitindo a verificação sistemática da existência ou não do delito em cada caso concreto.

Segundo Couto e Ferreira (2022), o fato típico corresponde à adequação da conduta humana ao tipo penal previsto em lei. Para sua configuração, exige-se a presença de elementos objetivos e subjetivos, tais como a ação ou omissão, o resultado, o nexo causal e o dolo ou a culpa, quando exigidos pelo tipo. A tipicidade

representa o primeiro juízo de análise da conduta, delimitando o campo de incidência do direito penal.

Superada a análise da tipicidade, passa-se à verificação da ilicitude. O fato típico será considerado ilícito quando contrariar o ordenamento jurídico como um todo, inexistindo causas legais de exclusão da antijuridicidade. A ilicitude expressa o caráter contrário ao Direito da conduta, sendo afastada apenas nas hipóteses em que o próprio sistema jurídico autoriza o comportamento, como ocorre nas excludentes legais (FERREIRA JUNIOR, 2023).

O terceiro elemento da estrutura clássica do crime é a culpabilidade, que consiste no juízo de reprovação pessoal da conduta ilícita. Segundo Reis e Souza (2025), a culpabilidade avalia se o agente pode ser responsabilizado pelo fato praticado, considerando sua imputabilidade, a possibilidade de conhecimento da ilicitude e a exigibilidade de conduta diversa. Trata-se de etapa indispensável para a imposição da sanção penal.

Essa estrutura tripartida visa garantir racionalidade e segurança jurídica na aplicação do direito penal. Ao exigir a presença cumulativa dos três elementos, o sistema penal estabelece critérios objetivos e subjetivos para a responsabilização, evitando punições arbitrárias e assegurando a observância dos princípios fundamentais do ordenamento jurídico (GIORGI JUNIOR, 2016).

2.8 A DIFICULDADE DE APLICAÇÃO DO DIREITO PENAL TRADICIONAL AOS CRIMES DIGITAIS

A aplicação do direito penal tradicional aos crimes digitais revela um conjunto de desafios que decorrem, sobretudo, da incompatibilidade entre os pressupostos clássicos do sistema penal e as características próprias do ambiente digital. O modelo penal foi estruturado para regular condutas praticadas em contextos físicos, territorialmente delimitados e passíveis de identificação direta dos agentes, elementos que nem sempre se fazem presentes na criminalidade contemporânea (ARAÚJO, 2024).

De acordo Flores (2025), os tipos penais tradicionais foram concebidos a partir de uma realidade social marcada por relações predominantemente físicas e por condutas praticadas em espaços territorialmente delimitados, a descrição típica dessas normas baseia-se em elementos materiais e circunstâncias concretas que

nem sempre encontram correspondência no ambiente digital, desta forma, essa estrutura normativa revela limitações quando aplicada aos crimes praticados por meio de sistemas informáticos.

Ainda segundo o autor a criminalidade digital caracteriza-se pela imaterialidade das condutas e pela utilização de meios tecnológicos que não estavam previstos no momento da elaboração dos tipos penais clássicos. Muitas infrações cometidas no ambiente virtual não se ajustam de forma precisa às descrições legais existentes, exigindo interpretações extensivas para viabilizar a punição (FLORES, 2025).

Tal prática, contudo, encontra limites nos princípios da legalidade e da tipicidade. A inadequação dos tipos penais tradicionais também se manifesta na dificuldade de enquadramento de condutas que envolvem múltiplos agentes e sistemas automatizados. A atuação em rede, típica dos crimes digitais, compromete a aplicação de conceitos clássicos de autoria e participação, previstos para contextos em que a conduta criminosa é facilmente atribuível a um sujeito determinado (MARTINS, 2024).

Além disso, muitos tipos penais tradicionais não contemplam a proteção adequada de bens jurídicos diretamente relacionados ao ambiente digital, como a segurança da informação e a integridade dos sistemas informáticos. A ausência de previsão específica para essas situações resulta em lacunas normativas que dificultam a repressão penal eficaz e comprometem a tutela dos interesses lesados (FÉRES, 2021).

A tentativa de adaptar os tipos penais clássicos às novas formas de criminalidade digital pode gerar insegurança jurídica. A ampliação interpretativa das normas penais, ainda que motivada pela necessidade de repressão às condutas ilícitas, pode violar garantias fundamentais do acusado e fragilizar o sistema penal. Essa tensão evidencia a insuficiência do modelo tradicional frente às transformações tecnológicas (MELO, 2024).

O princípio da territorialidade constitui um dos fundamentos clássicos da aplicação da lei penal no espaço, vinculando a incidência da norma ao território do Estado. Tal critério mostrou-se historicamente adequado a uma realidade social em que as condutas criminosas ocorriam em espaços físicos claramente delimitados. No entanto, diante da expansão do ciberespaço, esse paradigma enfrenta limitações significativas (CORRÊA; MARQUES, 2016).

Os crimes digitais são frequentemente praticados em ambientes virtuais que não se submetem a fronteiras geográficas definidas. A conduta ilícita pode envolver agentes localizados em diferentes países, servidores hospedados em territórios distintos e vítimas situadas em múltiplas jurisdições. Essa dispersão espacial dificulta a identificação do local de ocorrência do crime, elemento essencial para a aplicação do princípio da territorialidade (GOMES; MEDRADO; GAMA, 2024).

A ausência de um espaço físico determinado no ciberespaço compromete a definição da competência jurisdicional e a aplicação da lei penal adequada. A determinação do lugar do crime torna-se complexa, uma vez que a execução, o resultado e os efeitos da conduta podem ocorrer em locais diversos. Tal situação gera conflitos de competência e insegurança jurídica, tanto para os órgãos de persecução penal quanto para os indivíduos envolvidos (PRESTES, 2020).

Além disso, a aplicação rígida do princípio da territorialidade pode resultar na impunidade de determinadas condutas ilícitas praticadas no ambiente digital. A dificuldade de estabelecer vínculos territoriais claros limita a atuação estatal e compromete a efetividade da repressão penal, sobretudo quando inexistem mecanismos eficientes de cooperação internacional (FIGUEIREDO, 2025).

Segundo Castro (2023), a identificação da autoria e da materialidade constitui etapa essencial para a responsabilização penal, uma vez que permite atribuir a conduta ilícita a um sujeito determinado e comprovar a ocorrência do fato criminoso. No âmbito dos crimes digitais, contudo, esses elementos assumem contornos particularmente complexos, em razão das características próprias do ambiente virtual.

A autoria nos crimes digitais é frequentemente dificultada pela possibilidade de anonimato proporcionada pelas tecnologias da informação. O uso de perfis falsos, redes privadas virtuais, sistemas de criptografia e mecanismos de ocultação de endereço eletrônico compromete a identificação direta do agente. Essas ferramentas dificultam o rastreamento das ações praticadas no ambiente digital, exigindo conhecimentos técnicos especializados e cooperação entre diferentes instituições (OLIVEIRA; CUNHA; SILVA, 2025).

Além disso, a atuação em rede e a utilização de sistemas automatizados tornam mais complexa a atribuição da conduta a um único agente. Em muitos casos, os crimes digitais envolvem múltiplos sujeitos, distribuídos em diferentes localidades, o que dificulta a individualização da responsabilidade penal. Essa realidade desafia

os conceitos clássicos de autoria e participação previstos no direito penal tradicional (MAIA, 2017).

A materialidade dos crimes digitais também apresenta obstáculos específicos. Diferentemente dos delitos praticados no espaço físico, nos quais a prova material é geralmente tangível, os crimes digitais deixam vestígios imateriais, muitas vezes voláteis e passíveis de rápida alteração ou eliminação. Registros eletrônicos, logs de acesso e dados armazenados em sistemas digitais podem ser facilmente apagados ou manipulados (BARROS, 2023).

Como aponta Cordeiro e Morais (2024), a fragilidade da prova digital exige procedimentos técnicos rigorosos para sua coleta, preservação e análise. A ausência de métodos adequados pode comprometer a autenticidade e a integridade das informações, inviabilizando sua utilização no processo penal. Essa situação impacta diretamente a comprovação da materialidade do delito e a formação do convencimento judicial.

Segundo Lira (2018), a evolução tecnológica ocorre de forma acelerada e contínua, impulsionada pela constante inovação nos sistemas digitais e pela ampliação do uso da internet em diferentes esferas da vida social. Esse ritmo dinâmico de transformação contrasta com o processo legislativo, que, por sua própria natureza, apresenta caráter mais lento e formal, exigindo debates, deliberações e procedimentos institucionais complexos.

A lentidão legislativa resulta, frequentemente, em lacunas normativas diante de práticas criminosas emergentes no ambiente digital. Condutas potencialmente lesivas permanecem sem tipificação específica por longos períodos, limitando a atuação estatal e comprometendo a efetividade da tutela penal. Essa situação evidencia a dificuldade do ordenamento jurídico em acompanhar as transformações impostas pela sociedade da informação (FLORES, 2025).

Como aponta Deolindo (2025), a tentativa de responder rapidamente às demandas sociais pode levar à elaboração de normas penais insuficientemente debatidas ou tecnicamente inadequadas, a produção legislativa apressada, sem análise aprofundada dos impactos tecnológicos, pode gerar tipos penais imprecisos ou de difícil aplicação prática, aumentando a insegurança jurídica.

A tensão entre a velocidade da tecnologia e a lentidão legislativa expõe um dos principais desafios do direito penal contemporâneo. A necessidade de estabilidade normativa confronta-se com a exigência de adaptação constante às novas formas de

criminalidade digital. Esse cenário reforça a importância de estratégias legislativas mais flexíveis, bem como de interpretações jurídicas capazes de dialogar com a realidade tecnológica, sem comprometer as garantias fundamentais (ASSUNÇÃO, 2019).

2.9 EVOLUÇÃO LEGISLATIVA BRASILEIRA NO COMBATE AOS CRIMES DIGITAIS

A evolução da criminalidade digital impôs ao ordenamento jurídico brasileiro a necessidade de adaptação normativa frente às transformações decorrentes do avanço tecnológico. Durante longo período, o sistema penal nacional mostrou-se insuficiente para lidar com condutas ilícitas praticadas no ambiente digital, em razão da inexistência de tipos penais específicos e da inadequação das normas tradicionais às novas formas de criminalidade (MORAIS, 2025).

Inicialmente, os crimes praticados por meio de tecnologias da informação eram enquadrados, de forma subsidiária, em tipos penais clássicos, elaborados para regular condutas ocorridas no espaço físico. Essa prática interpretativa evidenciou limitações relevantes, especialmente diante das particularidades técnicas e da complexidade das infrações digitais. A ausência de legislação específica contribuiu para a insegurança jurídica e para dificuldades na repressão penal dessas condutas (BICALHO, 2024).

De acordo com Araújo Filho (2025), com o aumento da incidência de crimes digitais e a ampliação do debate público acerca da proteção de dados, da privacidade e da segurança da informação, o legislador brasileiro passou a adotar medidas normativas voltadas ao enfrentamento dessas práticas. A criação de leis específicas representou um avanço no reconhecimento da relevância jurídica do ambiente digital e na tentativa de adequar o sistema penal à realidade tecnológica.

Entretanto, a evolução legislativa no combate aos crimes digitais não ocorreu de forma linear ou suficiente. Embora tenham sido editadas normas importantes, persistem lacunas e desafios relacionados à efetividade da tutela penal e à compatibilidade das leis existentes com os princípios fundamentais do direito penal. A análise desse processo legislativo revela tanto avanços quanto limitações na resposta estatal à criminalidade digital (MACHADO, 2023).

Como destaca Martins (2024), o surgimento das primeiras práticas criminosas no ambiente digital ocorreu em um contexto no qual o ordenamento penal brasileiro não dispunha de normas específicas voltadas à repressão dessas condutas. O código

penal, elaborado em um período histórico marcado por relações sociais predominantemente físicas, não previa situações relacionadas ao uso de sistemas informáticos ou à prática de delitos no ciberespaço, condutas praticadas por meio da internet eram enquadradas, de forma analógica ou extensiva, em crimes já existentes, como estelionato, dano ou violação de correspondência. Essa prática evidenciava a tentativa de adaptar o sistema penal a uma realidade não prevista pelo legislador originário.

Entretanto, a ausência de legislação específica gerou insegurança jurídica e dificuldades práticas na persecução penal. A aplicação de tipos tradicionais a condutas digitais nem sempre se mostrava adequada, especialmente diante das exigências impostas pelos princípios da legalidade e da tipicidade. Muitas práticas ilícitas permaneciam sem resposta penal eficaz, em razão da inexistência de previsão normativa clara (ARAÚJO, 2024).

Dessa forma, o vácuo legislativo inicial no ordenamento penal brasileiro evidencia o descompasso entre a evolução tecnológica e a capacidade de resposta normativa do Estado. Esse cenário contribuiu para a percepção da necessidade de criação de legislações específicas voltadas ao combate aos crimes digitais, tema que será analisado nos tópicos subsequentes (VELOSO FILHO, 2025).

A promulgação do Marco Civil da Internet, por meio da Lei nº 12.965/2014, representou um marco normativo relevante na regulamentação do uso da internet no Brasil. Diferentemente das leis penais tradicionais, esse diploma não possui caráter incriminador, mas estabelece princípios, garantias, direitos e deveres para o uso da rede, consolidando uma base jurídica para a atuação estatal no ambiente digital, ao dispor expressamente que “esta Lei estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria” (BRASIL, 2014).

O Marco Civil da Internet foi concebido com enfoque predominantemente civil e constitucional, priorizando a proteção de direitos fundamentais, como a liberdade de expressão, a privacidade e a proteção de dados pessoais. Ainda assim, seus dispositivos produzem reflexos significativos no âmbito penal, especialmente no que se refere à investigação e à persecução de crimes praticados no ambiente digital (SILVA, 2024).

Um dos principais reflexos penais do Marco Civil reside na regulamentação da guarda e do fornecimento de registros de conexão e de acesso a aplicações de internet. A lei estabelece critérios e prazos para a conservação desses dados pelos provedores, bem como condiciona seu fornecimento à ordem judicial. Essas disposições impactam diretamente a produção de provas em processos penais envolvendo crimes digitais (BODIN, 2017).

Outro aspecto relevante refere-se à responsabilização dos provedores de aplicações de internet. O Marco Civil estabelece que os provedores somente podem ser responsabilizados civilmente por conteúdos gerados por terceiros mediante descumprimento de ordem judicial específica. Embora essa previsão tenha natureza civil, ela influencia a dinâmica da responsabilização penal, ao delimitar o papel dos intermediários digitais no contexto das infrações praticadas online.

De acordo com Rocha (2025), o Marco Civil da Internet não soluciona de forma plena os desafios enfrentados pelo direito penal no combate aos crimes digitais pois a ausência de tipificações penais específicas e a dependência de legislação complementar evidenciam que seus reflexos penais são indiretos e limitados. Ainda assim, o diploma representa importante instrumento normativo de apoio à persecução penal, ao fornecer parâmetros legais para a obtenção de provas e para a proteção de direitos no ambiente digital.

A Lei Geral de Proteção de Dados Pessoais, instituída pela Lei nº 13.709/2018, representa avanço significativo na regulamentação do tratamento de dados pessoais no ordenamento jurídico brasileiro. Inspirada em modelos internacionais de proteção de dados, a LGPD foi elaborada com o objetivo de assegurar direitos fundamentais relacionados à liberdade, à privacidade e ao livre desenvolvimento da personalidade da pessoa natural.

Conforme dispõe o artigo 1º da Lei nº 13.709/2018:

Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (BRASIL, 2018).

Embora possua natureza predominantemente administrativa e civil, a LGPD produz reflexos relevantes no âmbito penal, especialmente no contexto dos crimes digitais. A lei estabelece princípios e regras para a coleta, o armazenamento, o uso e

o compartilhamento de dados pessoais, impondo limites jurídicos às atividades realizadas no ambiente digital. Tais disposições impactam diretamente a forma como determinadas condutas ilícitas são compreendidas e enfrentadas pelo sistema penal (SANTOS; BOTELHO, 2023).

A proteção de dados pessoais como bem jurídico reforça a relevância penal de condutas que envolvem o uso indevido de informações pessoais. Práticas como o vazamento de dados, o acesso não autorizado a informações sensíveis e o tratamento irregular de dados passaram a ser analisadas sob uma nova perspectiva normativa, ainda que nem todas estejam tipificadas como crimes de forma expressa (AVELINO, 2024).

A ausência de tipificações penais específicas na LGPD evidencia, contudo, uma limitação do diploma legal no combate direto aos crimes digitais. A lei opta por um modelo sancionatório predominantemente administrativo, o que restringe sua atuação no campo penal e mantém a dependência de normas incriminadoras previstas em outros diplomas legais (CAMARGO, 2022).

3 METODOLOGIA

A metodologia adotada neste trabalho foi estruturada de modo a garantir coerência entre o problema de pesquisa, os objetivos propostos e os instrumentos utilizados para a sua análise. Trata-se de uma pesquisa de abordagem qualitativa, de caráter exploratório e descritivo, desenvolvida por meio de revisão bibliográfica, complementada pela análise de documentos legais, doutrinários e jurisprudenciais relacionados aos crimes digitais e ao direito penal tradicional.

A dimensão exploratória justifica-se pela necessidade de ampliar a compreensão acerca das particularidades da criminalidade digital e dos desafios que ela impõe ao modelo penal clássico, enquanto o caráter descritivo permite identificar, organizar e expor os principais aspectos jurídicos envolvidos no fenômeno estudado. Quanto aos procedimentos, a pesquisa classifica-se como bibliográfica e documental, tomando por base obras doutrinárias, artigos científicos, legislação e entendimentos jurisprudenciais pertinentes ao tema.

3.1 TIPO DE PESQUISA

O presente estudo classifica-se como pesquisa bibliográfica, de abordagem qualitativa e de caráter exploratório e descritivo. É bibliográfica porque se fundamenta na análise de obras doutrinárias, textos normativos, produções científicas e decisões judiciais relacionadas à dificuldade de aplicação do direito penal tradicional aos crimes digitais.

Possui abordagem qualitativa por priorizar a interpretação dos conceitos, categorias e argumentos jurídicos envolvidos no tema, sem recorrer a técnicas estatísticas ou mensuração numérica.

Este estudo evidencia pesquisa com abordagem qualitativa, que de acordo com os autores Dias e Silva (2010, p. 67): “a pesquisa qualitativa envolve o uso de dados qualitativos obtidos em entrevista, documentos, e observações para compreensão e explicação de fenômenos.” Desta maneira, este tipo de pesquisa demonstra os dados de forma clara, onde o pesquisador contribua e alcance as informações e as esclareça.

Deste modo, a pesquisa com abordagem qualitativa é traduzida por aquilo que não pode ser mensurável, ou seja, algo que pode medir qualquer grandeza que pode

passar por uma contagem, pois a realidade e o sujeito são elementos indissociáveis, ou seja, que não se pode dividir em partes. “Tratando os dados de forma qualitativa, estes foram codificados e apresentados de forma mais estruturada e analisada” (DIAS; SILVA, 2010, p. 287).

Apresenta, ainda, caráter exploratório e descritivo, por buscar maior aprofundamento em uma temática marcada por constante transformação tecnológica, teórica e legislativa, e descritivo, por sistematizar os principais conceitos, classificações, princípios e dificuldades relacionados à aplicação do direito penal à criminalidade digital.

Sendo utilizadas as pesquisas exploratória e descritiva, em que segundo Severino (2007), a pesquisa exploratória busca apenas levantar informações sobre um determinado objeto, delimitando assim um campo de trabalho, mapeando as condições de manifestação desse objetivo. De acordo com Cervo e Bervian (2002), a pesquisa descritiva investiga de forma detalhada onde passa a correlatar cada fato ocorrido sem serem manipulados.

3.2 COLETA DE DADOS

A coleta de dados foi realizada por meio de levantamento bibliográfico e documental, com a finalidade de reunir materiais relevantes para a análise da dificuldade de aplicação do direito penal tradicional aos crimes digitais. No âmbito bibliográfico, foram selecionados livros, artigos científicos, teses, dissertações e ensaios que abordam temas como sociedade da informação, crimes digitais, direito penal tradicional, princípios penais e evolução legislativa. Esse levantamento forneceu o embasamento teórico necessário à compreensão do objeto de estudo e à definição das categorias analíticas empregadas na pesquisa.

Neste estudo foi utilizada a pesquisa bibliográfica para a fundamentação e ponderação de diversos autores renomados, com diversos artigos e livros, portanto é válido destacar que é de suma importância para sanar qualquer questionamento sobre o tema. Segundo Severino (2007, p. 122):

A pesquisa bibliográfica é aquela que se realiza a partir do registro disponível, decorrente de pesquisas anteriores, em documentos impressos, como livros, artigos, teses e etc. Utiliza-se de dados ou de categorias teóricas já trabalhados por outros pesquisadores e devidamente registrados [...].

Em seus demasiados meios, a referida pesquisa é estritamente de caráter exploratório e descritivo, pois visa levantar informações sobre o assunto abordado, delimitando assim o objeto em questão, com o intuito de identificar o fenômeno abordado.

No âmbito documental, a coleta concentrou-se no exame de textos normativos, especialmente o Código Penal, leis penais especiais e diplomas relacionados à internet e à proteção de dados, bem como em decisões judiciais e documentos institucionais pertinentes ao tema. Esses documentos foram selecionados por sua relevância para a compreensão da resposta do sistema jurídico aos delitos praticados em ambiente virtual, permitindo identificar, no plano normativo e interpretativo, os principais entraves à aplicação do direito penal tradicional diante da criminalidade digital.

3.3 TÉCNICAS DE ANÁLISE DOS DADOS

Os dados obtidos por meio da revisão bibliográfica e da pesquisa bibliográfica são analisados por meio de análise qualitativa de conteúdo, com organização do material por eixos temáticos, tais como: sociedade da informação, conceito e classificação dos crimes digitais, princípios do direito penal tradicional e dificuldades de aplicação das normas penais ao ciberespaço.

Adota-se, ainda, a interpretação sistemática das normas jurídicas, buscando compreender os dispositivos legais em sua relação com o conjunto do ordenamento penal e com diplomas correlatos, como o Marco Civil da Internet e a Lei Geral de Proteção de Dados.

Realiza-se o confronto entre o direito penal tradicional e os crimes digitais, comparando os pressupostos da dogmática penal clássica com as peculiaridades da criminalidade digital, a fim de evidenciar limites, tensões e necessidades de atualização normativa e dogmática.

3.4 CRITÉRIOS DE INCLUSÃO E EXCLUSÃO

Para a composição do corpus da pesquisa, foram adotados critérios de inclusão e exclusão com a finalidade de garantir coerência entre o material analisado e os objetivos do estudo. Como critérios de inclusão, selecionaram-se obras doutrinárias,

artigos científicos, dissertações, teses, textos normativos, decisões jurisprudenciais e documentos institucionais diretamente relacionados à sociedade da informação, aos crimes digitais, ao direito penal tradicional, aos princípios penais e à evolução legislativa brasileira sobre a matéria.

Também foram incluídos materiais que apresentassem pertinência temática com o problema de pesquisa, especialmente aqueles voltados à discussão da tipicidade, da territorialidade, da autoria, da materialidade e das dificuldades de repressão penal no ambiente digital.

Como critérios de exclusão, foram desconsiderados materiais que, embora tratassem de tecnologia ou criminalidade em sentido amplo, não apresentassem relação direta com a dificuldade de aplicação do direito penal tradicional aos crimes digitais. Também foram excluídos textos repetidos, publicações sem relevância científica ou jurídica para o tema, documentos sem conexão com o recorte proposto e materiais que abordassem a criminalidade digital apenas de forma superficial, sem contribuição efetiva para a análise dogmática, normativa ou jurisprudencial desenvolvida neste trabalho.

4 RESULTADOS E DISCUSSÃO

Com base no material científico selecionado e após a leitura dos artigos, os resultados e as discussões foram organizados de modo a permitir uma análise progressiva do problema investigado. Inicialmente, buscou-se compreender de que maneira a sociedade da informação, a ampliação do uso da internet e a virtualização das relações sociais contribuíram para a expansão dos crimes digitais, considerando que o ambiente virtual passou a favorecer novas formas de lesão a bens jurídicos já tutelados pelo direito, além de viabilizar práticas ilícitas marcadas pela rapidez, dispersão e alcance transnacional.

Em seguida, a análise voltou-se aos fundamentos do direito penal tradicional aplicáveis ao ambiente digital, com ênfase nas dificuldades encontradas para a repressão penal dessas condutas. Nesse ponto, foram observados os principais entraves apontados pela literatura, especialmente quanto à tipicidade, à territorialidade, à identificação da autoria, à comprovação da materialidade e à obtenção, preservação e validade da prova digital, aspectos que demonstram a insuficiência de soluções construídas exclusivamente a partir dos referenciais clássicos do sistema penal.

Por fim, os resultados e as discussões foram direcionados à avaliação da evolução legislativa brasileira no enfrentamento dos crimes digitais, examinando se os avanços normativos recentes têm sido suficientes para responder às especificidades do ciberespaço. A partir disso, buscou-se refletir sobre as limitações estruturais do modelo penal clássico diante das novas dinâmicas delitivas e sobre a necessidade de respostas investigativas, probatórias e legislativas mais adequadas à criminalidade contemporânea.

Quadro 1 - Comparativo de estudos analisando os crimes digitais e a dificuldade de aplicação do direito penal tradicional.

Título	Autores e Ano	Objetivo	Principais resultados
Persecução penal digital: a prova na era da informação	Arigony; Botton; Arigony, (2025)	Analisar o impacto das provas digitais na resolução de crimes e propor melhorias para a investigação criminal no contexto digital, a partir de um estudo de caso de homicídio ocorrido em Santa Maria/RS.	O artigo conclui que as ferramentas tecnológicas foram decisivas para a coleta de evidências e identificação dos autores; também destaca que a validade da prova digital depende de autorização judicial, preservação da cadeia de custódia e respeito à LGPD e ao CPP, além da necessidade de atualização constante dos profissionais e das práticas investigativas.

Título	Autores e Ano	Objetivo	Principais resultados
Função ‘hash’ e a integridade da prova digital	Fisberg, (2025)	Examinar a função hash como instrumento de garantia da integridade da prova digital, analisando seus fundamentos técnicos, suas limitações e sua aplicação na cadeia de custódia, com apoio em estudo interdisciplinar e jurisprudência do STJ.	O estudo mostra que o hash é técnica relevante para verificar a integridade de dados digitais, mas não é infalível nem suficiente por si só; sua eficácia é relativa, depende de rigor técnico e conhecimento especializado, e a jurisprudência revela divergências quanto ao seu uso, o que reforça a necessidade de documentação rigorosa da cadeia de custódia.
Crimes cibernéticos	Maia; Costa, (2023)	Analisar a evolução histórica dos crimes cibernéticos, a legislação aplicável e a importância do poder público na prevenção e punição desses delitos.	O artigo demonstra que os crimes cibernéticos passaram de ocorrências isoladas para ameaça global e economicamente lucrativa; também conclui que o combate a essas práticas exige legislação dinâmica, atuação estatal proativa, cooperação internacional e colaboração entre setor público e privado.
Crimes cibernéticos: panorama legislativo	Montel; Paiva, (2024)	Apresentar a incidência dos crimes cibernéticos sob o panorama legislativo brasileiro, expondo seus conceitos, tipificações e o desenvolvimento das principais normas nacionais sobre o tema.	O trabalho conclui que o Brasil avançou com marcos como a Lei Carolina Dieckmann, o Marco Civil da Internet, a LGPD e a Lei nº 14.155/2021, mas ainda enfrenta dificuldades quanto à aplicação efetiva dessas normas, à capacitação técnica das instituições e à atualização legislativa diante de novas modalidades criminosas, o que revela a necessidade de medidas mais assertivas e de contínuo aperfeiçoamento jurídico.
A competência territorial nas fraudes bancárias praticadas pela internet	Otreira, (2020)	Identificar, nas investigações de fraudes bancárias praticadas pela internet, as dificuldades geradas pelo entendimento jurisprudencial que fixa a competência territorial com base na localização da agência bancária vinculada aos envolvidos.	O artigo conclui que esse critério territorial tradicional prejudica a investigação, sobretudo porque vítima, autor e instituição financeira frequentemente se encontram em lugares distintos; por isso, propõe que a competência seja fixada no local de domicílio ou residência da vítima, por ser o parâmetro mais adequado à dinâmica dos delitos cibernéticos e à rápida apuração dos vestígios.
Os crimes cibernéticos no ordenamento jurídico brasileiro: investigação criminal e desafios	Queiroz, (2024)	Analisar os tipos de crimes cibernéticos, os modos de investigação criminal, suas especificidades e desafios, com destaque para o Marco Civil da Internet e a Convenção de Budapeste como instrumentos de investigação.	O artigo destaca a necessidade de preservação imediata dos dados digitais em razão da volatilidade da prova, ressalta a importância da qualificação das autoridades para investigação cibernética e aponta que a Convenção de Budapeste trouxe medidas mais eficazes e céleres para obtenção de prova digital; ao mesmo tempo, evidencia entraves como anonimização, compartilhamento de IP e uso de CGNAT, defendendo a necessidade de legislação penal e processual mais específica.

Título	Autores e Ano	Objetivo	Principais resultados
O malware como meio de obtenção de prova e a sua implementação no ordenamento jurídico brasileiro	Ribeiro; Cordeiro; Fumach, (2022)	Analisar os principais problemas ligados ao uso de malware como meio de obtenção de prova na investigação criminal e verificar se sua utilização é juridicamente possível no Brasil.	O estudo conclui que, diante da legislação vigente, o uso de malware não é admissível no ordenamento brasileiro, especialmente por seu elevado grau de invasividade e por afetar diversos direitos fundamentais e garantias processuais; ainda assim, o artigo apresenta parâmetros que poderiam orientar futura regulamentação específica da medida.
A obtenção das provas digitais no processo penal demanda uma disciplina jurídica própria? Uma análise do conceito, das características e das peculiaridades das provas digitais	Saad; Rossi; Partata, (2024)	Responder se a obtenção de provas digitais no processo penal brasileiro demanda disciplina jurídica própria, analisando conceito, características, direitos fundamentais atingidos e formas de obtenção desses dados.	O artigo conclui positivamente que a prova digital exige disciplina jurídica própria, com hipóteses, requisitos e procedimentos específicos; demonstra ainda que as características dessas provas, como imaterialidade, volatilidade e necessidade de intermediação técnica, impõem cuidados especiais de autenticidade, confiabilidade e cadeia de custódia, e que o regime atual é insuficiente, sobretudo em casos de hacking e malware.

Fonte: Dados da pesquisa (2025).

A partir da sistematização dos artigos no quadro acima, observa-se que a criminalidade digital se desenvolve no interior de uma sociedade cada vez mais marcada pela informatização das relações, pela circulação instantânea de dados e pela ampliação das interações em ambiente virtual.

Nesse cenário, os crimes cibernéticos deixam de representar episódios isolados e passam a assumir posição de destaque no debate jurídico contemporâneo, não apenas pela multiplicidade de condutas que podem ser praticadas por meio da internet, mas também pela expansão de riscos relacionados ao anonimato, à transnacionalidade e à rapidez com que as infrações se propagam no meio digital.

Ao mesmo tempo, a literatura analisada evidencia que a evolução legislativa brasileira, embora relevante, ainda não eliminou as dificuldades práticas e normativas envolvidas na repressão dessas condutas.

Nesse contexto, a discussão proposta neste capítulo parte da compreensão de que a aplicação do direito penal tradicional aos crimes digitais encontra limites importantes, especialmente quando se examinam questões ligadas à tipicidade, à definição da competência, à identificação da autoria e à produção da prova digital. Isso ocorre porque os vestígios informáticos possuem características próprias, como

volatilidade, imaterialidade e dependência de procedimentos técnicos específicos de preservação, o que exige maior cautela investigativa e, em muitos casos, disciplina jurídica mais precisa.

Desse modo, os resultados e as discussões a seguir procuram demonstrar que o enfrentamento adequado da criminalidade digital depende não apenas da existência de tipos penais e leis especiais, mas também do aperfeiçoamento dos instrumentos probatórios, da capacitação dos agentes estatais e da compatibilização entre eficiência investigativa e proteção dos direitos fundamentais.

4.1 SOCIEDADE DA INFORMAÇÃO, VIRTUALIZAÇÃO DAS RELAÇÕES SOCIAIS E EXPANSÃO DOS CRIMES DIGITAIS

A compreensão dos crimes digitais exige, antes de tudo, o reconhecimento de que a sociedade contemporânea passou por profundas transformações com o avanço da internet e das tecnologias da informação. A ampliação da conectividade, a circulação intensa de dados e a incorporação dos meios digitais às atividades cotidianas alteraram significativamente as formas de comunicação, consumo, trabalho e interação social, consolidando um cenário em que grande parte da vida em sociedade passou a se desenvolver em ambiente virtual.

Nesse novo contexto, o espaço digital deixou de ser apenas um instrumento de facilitação da vida moderna e passou também a abrigar novas formas de conflito, exposição e lesão a bens jurídicos. A mesma estrutura que favorece rapidez, alcance e interação em rede também amplia vulnerabilidades, possibilitando que práticas ilícitas se adaptem com facilidade às dinâmicas do meio virtual. Por isso, a análise deste tópico parte da relação entre sociedade da informação, virtualização das relações sociais e crescimento da criminalidade digital, a fim de compreender como o desenvolvimento tecnológico contribuiu para a expansão dessas condutas.

Maia e Costa (2023) demonstram que os crimes cibernéticos passaram, ao longo do tempo, de ocorrências isoladas para uma ameaça global, acompanhando o crescimento da internet e da tecnologia. Os autores explicam que a evolução histórica desses delitos está ligada à própria transformação do mundo contemporâneo, cada vez mais interconectado e dependente de recursos digitais. Além disso, destacam que as motivações dos agentes também se modificaram, deixando de se limitar à

curiosidade técnica e passando a envolver enriquecimento ilícito, espionagem e outras práticas com alto potencial lesivo.

A partir dessa leitura, percebe-se que a expansão dos crimes digitais está diretamente relacionada ao fortalecimento da sociedade da informação. Quanto maior é a presença da internet nas atividades humanas, maiores também se tornam as possibilidades de utilização indevida dessas ferramentas. Assim, o estudo de Maia e Costa (2023) ajuda a compreender que a criminalidade digital não surgiu à margem da evolução tecnológica, mas dentro dela, como uma consequência do próprio processo de informatização da vida social. Esse entendimento serve de base para observar, no parágrafo seguinte, que a ampliação das relações sociais no ambiente digital produziu benefícios, mas também novas vulnerabilidades, como apontam Montel e Paiva (2024).

Montel e Paiva (2024) afirmam que a crescente expansão das relações sociais, econômicas e culturais no ambiente tecnológico trouxe diversos benefícios, mas também abriu espaço para o surgimento de práticas ilícitas. As autoras destacam que os crimes cibernéticos abrangem condutas como invasões de sistemas, fraudes eletrônicas, divulgação indevida de dados pessoais e disseminação de notícias falsas. O estudo também enfatiza que a alta utilização da tecnologia no cotidiano impulsionou o sistema jurídico-legislativo a se adaptar a essa nova realidade, marcada por constante transformação e renovação.

O argumento de Montel e Paiva (2024) é relevante porque mostra que a virtualização das relações sociais não deve ser vista apenas como avanço técnico, mas como mudança estrutural na forma de viver, comunicar-se e interagir. Quando as atividades do cotidiano passam a depender de dispositivos conectados, o ambiente digital também se torna um espaço propício para a prática de ilícitos. Desse modo, a expansão dos crimes digitais acompanha a mesma lógica que impulsiona a sociedade da informação: rapidez, conectividade, circulação de dados e facilidade de acesso. Esse raciocínio se conecta ao que Arigony, Botton e Arigony (2025) observam ao tratar da passagem de um modelo analógico para um contexto predominantemente digital.

Arigony, Botton e Arigony (2025) partem da ideia de que a sociedade contemporânea foi profundamente impactada por uma revolução técnico-científica, que alterou o paradigma da interação social e deslocou as relações humanas de um modelo analógico para um contexto predominantemente digital. Os autores mostram que esse novo cenário exige adaptações também no campo das investigações

criminais, sobretudo porque o aumento dos crimes cibernéticos e a relevância crescente das provas digitais demandam modernização das práticas investigativas. O estudo ainda evidencia que as ferramentas tecnológicas foram cruciais para coleta de evidências e identificação de autores em casos concretos.

A contribuição de Arigony, Botton e Arigony (2025) é importante porque evidencia que a virtualização das relações sociais não impactou apenas o modo como as pessoas convivem, mas também a forma como os crimes são praticados e investigados. Em um ambiente cada vez mais digital, os vestígios delitivos deixam de ser somente físicos e passam a se manifestar em redes sociais, dispositivos eletrônicos e registros informacionais. Assim, o crescimento da criminalidade digital deve ser compreendido juntamente com a ampliação dos meios tecnológicos que estruturam a vida cotidiana. Esse ponto abre espaço para a análise de Queiroz (2024), que aprofunda a ideia de que a internet, embora utilizada para finalidades lícitas, também se consolidou como campo fértil para a prática criminosa.

Queiroz (2024) observa que a internet é utilizada para múltiplas finalidades legítimas, como pesquisas, compras, operações financeiras, redes sociais e relacionamentos. Contudo, a autora destaca que esse mesmo ambiente também tem servido de campo fértil para a prática de crimes cibernéticos próprios e impróprios. O artigo mostra, ainda, que a popularização do acesso à internet e a expansão das redes sociais contribuíram para o aumento expressivo das vítimas, ao mesmo tempo em que a volatilidade da prova digital, a anonimização de dados e o compartilhamento de IP dificultam a identificação dos autores e o prosseguimento das investigações.

A análise de Queiroz (2024) permite perceber que a expansão dos crimes digitais acompanha a própria ampliação dos usos sociais da internet. À medida que o espaço virtual passa a concentrar atividades econômicas, sociais, afetivas e comunicacionais, ele também amplia as oportunidades para práticas ilícitas. Além disso, o artigo mostra que a criminalidade digital se fortalece em razão de características próprias do meio virtual, como rapidez, anonimato relativo e fragilidade probatória. Com isso, fica mais evidente que a sociedade da informação não apenas cria novas formas de convivência, mas também novos espaços de conflito e lesão.

Fisberg (2025) parte da constatação de que as últimas décadas foram marcadas por um movimento global de virtualização, no qual a informação, a comunicação e outras dimensões da vida social passaram a ser fortemente mediadas por tecnologias digitais. O autor demonstra que a chamada era da informação alterou

o próprio fenômeno criminal, pois conversas armazenadas, áudios, imagens, dados de localização, metadados e postagens em redes sociais passaram a integrar o universo dos vestígios relevantes no processo penal. Desse modo, o artigo evidencia que a expansão do ambiente digital repercute diretamente não apenas na prática dos delitos, mas também na forma como eles deixam rastros e podem ser reconstruídos juridicamente.

A contribuição de Fisberg (2025) é importante porque mostra que a virtualização das relações sociais não amplia somente as possibilidades de ação criminosa, mas também modifica a natureza do vestígio deixado pelo crime. Em uma sociedade cada vez mais estruturada por fluxos de dados, os acontecimentos juridicamente relevantes deixam de estar apenas no mundo físico e passam a se manifestar em registros digitais, muitas vezes dispersos e tecnicamente complexos. Assim, a expansão dos crimes digitais deve ser compreendida em conjunto com a digitalização da própria experiência humana. Esse raciocínio ajuda a entender, no parágrafo seguinte, como a virtualização também atingiu de forma intensa as relações econômicas e bancárias, como demonstra Otreira (2020).

O autor demonstra que o advento e a popularização da internet tornaram as comunicações mais dinâmicas e modificaram profundamente a forma como empresas e consumidores se relacionam. O autor destaca que esse fenômeno alcançou fortemente o setor bancário, especialmente com a expansão das *fintechs* e dos serviços financeiros realizados integralmente pela internet. Nesse cenário, parte expressiva dos crimes cibernéticos passou a envolver fraudes bancárias praticadas a distância, em contextos nos quais vítima, autor e instituição financeira se encontram, muitas vezes, em localidades distintas. O estudo também mostra que a lógica territorial tradicional encontra dificuldades diante dessa nova dinâmica, justamente porque as operações virtuais tornam o crime mais fluido e desterritorializado (OTREIRA, 2020).

A análise de Otreira (2020) evidencia que a sociedade da informação não transformou apenas a comunicação, mas também a circulação patrimonial e as relações de consumo. Quando serviços bancários, transferências e movimentações financeiras passam a ocorrer de forma remota, o ambiente digital também se converte em espaço privilegiado para a prática de fraudes. Com isso, a expansão dos crimes digitais revela-se ligada à própria desmaterialização das relações econômicas e à facilidade de agir à distância. Além disso, o artigo mostra que a virtualização das

relações sociais enfraquece referências clássicas do direito penal, como a definição espacial do fato, o que serve de ponte para a reflexão de Ribeiro, Cordeiro e Fumach (2022), que examinam como a evolução tecnológica impactou a própria seara processual-penal.

Ribeiro, Cordeiro e Fumach (2022) afirmam que a vertiginosa evolução das tecnologias de informação, com destaque para o desenvolvimento da internet, revolucionou a forma como as pessoas se comunicam, organizam suas tarefas e armazenam dados e informações. Os autores mostram que essa nova realidade atingiu inevitavelmente a seara penal, pois, de um lado, permitiu o surgimento de ilícitos tipicamente virtuais e ampliou o uso de meios digitais para crimes não exclusivamente virtuais; de outro, despertou o interesse do Estado em empregar instrumentos tecnológicos mais sofisticados para prevenção e repressão de delitos. O estudo deixa claro, portanto, que a expansão da criminalidade digital acompanha a própria reconfiguração tecnológica da vida social contemporânea.

A relevância desse artigo está em evidenciar que a sociedade da informação produz um duplo movimento: ao mesmo tempo em que amplia as possibilidades de prática criminosa, também pressiona o Estado a desenvolver novas estratégias investigativas. Isso significa que a virtualização das relações sociais não interfere apenas na ação do infrator, mas em todo o sistema de persecução penal. As tecnologias digitais, portanto, transformam simultaneamente o crime, a prova e a investigação. Essa percepção é essencial porque demonstra que os crimes digitais não são apenas novos delitos, mas expressão de uma mudança estrutural na forma como a vida social se organiza (RIBEIRO; CORDEIRO; FUMACH, 2022).

Saad, Rossi e Partata (2024) demonstram que a prova digital possui características próprias, como imaterialidade, volatilidade, desprendimento do suporte físico, suscetibilidade de clonagem e necessidade de intermediação técnica. Para os autores, essas particularidades mostram que os dados digitais não podem ser tratados como mera extensão dos meios probatórios tradicionais. O estudo conclui que a obtenção dessas provas demanda disciplina jurídica própria, justamente porque a crescente digitalização da vida social faz com que cada vez mais informações relevantes estejam armazenadas em dispositivos, sistemas e fluxos eletrônicos, exigindo procedimentos rigorosos para garantir autenticidade e confiabilidade.

A análise de Saad, Rossi e Partata (2024) evidencia que a expansão dos crimes digitais ocorre em um ambiente marcado pela centralidade dos dados e pela

fragilidade dos vestígios eletrônicos. Em uma sociedade na qual comunicação, consumo, trabalho e memória passam a ser registrados digitalmente, também os conflitos penais se deslocam para um terreno imaterial, técnico e altamente sensível. Assim, a virtualização das relações sociais favorece não apenas o surgimento de novos delitos, mas também a necessidade de novas respostas jurídicas. Em síntese, os autores permitem concluir que o crescimento dos crimes digitais acompanha a transformação da própria vida em sociedade, o que prepara, de forma natural, a passagem para o próximo tópico, voltado às limitações do direito penal tradicional diante dessas novas dinâmicas criminosas.

Ao longo da análise, observa-se que a expansão dos crimes digitais acompanha a própria reorganização da vida social em bases tecnológicas. A internet e os sistemas informáticos passaram a integrar relações pessoais, econômicas e institucionais, o que ampliou não apenas as possibilidades legítimas de comunicação e circulação de informações, mas também os meios de atuação criminosa. Nesse cenário, os delitos praticados no ambiente virtual revelam-se como expressão direta de uma sociedade cada vez mais conectada, rápida e desterritorializada.

Verifica-se, assim, que a virtualização das relações sociais favoreceu tanto o surgimento de novas modalidades delitivas quanto a adaptação de infrações já conhecidas ao meio digital, tornando mais complexa a sua prevenção e repressão. Com isso, fica evidenciado que o crescimento dos crimes digitais não pode ser dissociado da sociedade da informação, pois é justamente nesse ambiente de intensa circulação de dados, interações remotas e dependência tecnológica que essas práticas se fortalecem. Essa constatação conduz, de forma natural, ao exame seguinte, voltado às dificuldades de aplicação do direito penal tradicional diante das particularidades do ciberespaço.

4.2 DESAFIOS DO DIREITO PENAL TRADICIONAL FRENTE AOS CRIMES DIGITAIS: TIPICIDADE, PROVA, AUTORIA, TERRITORIALIDADE E INSUFICIÊNCIA LEGISLATIVA

A aplicação do direito penal tradicional aos crimes digitais encontra obstáculos relevantes, sobretudo porque o ambiente virtual apresenta características que nem sempre se ajustam com facilidade às categorias clássicas do sistema penal. A literatura examinada mostra que, embora o ordenamento brasileiro tenha avançado

com leis específicas e com a incorporação de instrumentos voltados à persecução penal no ciberespaço, ainda persistem dificuldades relacionadas ao enquadramento típico das condutas, à definição de competência, à identificação da autoria, à obtenção e preservação da prova digital e à própria suficiência do aparato legislativo diante da velocidade com que a criminalidade tecnológica se transforma.

Nessa perspectiva, antes do exame dos entraves específicos, é importante observar que a aplicação do direito penal tradicional aos crimes digitais continua orientada por fundamentos clássicos do sistema penal, como a legalidade, a tipicidade cerrada, a necessidade de prova idônea, a definição de competência e a individualização da conduta do agente. Ocorre que, no ambiente virtual, tais categorias passam a enfrentar tensões próprias, pois as condutas se manifestam de forma mais fluida, os vestígios assumem natureza imaterial e a identificação do autor nem sempre se dá por critérios convencionais, exigindo releitura desses referenciais diante das particularidades do ciberespaço.

Montel e Paiva (2024) demonstram que a legislação brasileira passou a conferir maior atenção aos crimes cibernéticos com a edição de marcos como a Lei nº 12.737/2012, o Marco Civil da Internet, a LGPD e a Lei nº 14.155/2021. As autoras destacam que esses diplomas foram importantes para enfrentar condutas praticadas no meio digital, especialmente invasões de dispositivos, fraudes eletrônicas e violações de dados. Ainda assim, o estudo mostra que, apesar desses avanços, a legislação continua encontrando dificuldades para acompanhar a rápida evolução das práticas criminosas, o que revela permanência de lacunas e necessidade de atualização contínua do sistema jurídico.

A leitura de Montel e Paiva (2024) permite compreender que o desafio da tipicidade, nos crimes digitais, não decorre apenas da ausência total de normas, mas da insuficiência de um modelo legislativo que frequentemente reage depois que as novas formas de delito já estão consolidadas. Em muitos casos, o direito penal clássico tenta adaptar tipos antigos a condutas praticadas em ambiente virtual, o que nem sempre produz resposta segura ou suficiente. Desse modo, embora haja avanço normativo, a expansão da criminalidade digital continua pressionando o legislador a rever categorias tradicionais e a lidar com infrações que assumem formas mutáveis, transnacionais e tecnologicamente sofisticadas.

Queiroz (2024) observa que os crimes cibernéticos podem ser próprios ou impróprios, o que já demonstra a complexidade do enquadramento jurídico dessas

condutas. A autora destaca que alguns delitos dependem necessariamente do ambiente informático, enquanto outros apenas utilizam a tecnologia como meio de execução, a exemplo de ameaça, racismo, estelionato e crimes contra a honra. O artigo ainda enfatiza que o ordenamento jurídico brasileiro não possui uma norma penal unificada para os crimes cibernéticos, estando os tipos dispersos em diferentes leis, além de apontar que a investigação criminal enfrenta entraves ligados à volatilidade da prova digital, à anonimização de dados, ao compartilhamento de IP e à carência de qualificação técnica das autoridades.

A análise de Queiroz (2024) é especialmente relevante porque mostra que os desafios do direito penal tradicional não se concentram apenas na punição, mas começam já na própria definição da conduta e prosseguem até a fase de investigação. A classificação entre crimes próprios e impróprios indica que o ambiente digital nem sempre cria delitos inteiramente novos; muitas vezes, ele reconfigura infrações já conhecidas, dificultando a delimitação do que realmente exige tipo penal autônomo e do que pode ser abrangido por figuras já existentes. Além disso, quando a autoria depende da correta identificação de rastros eletrônicos, a investigação passa a depender de conhecimentos técnicos, rapidez na preservação de dados e cooperação com provedores, o que evidencia a limitação de respostas baseadas apenas em categorias clássicas do processo penal.

Otreira (2020) examina especificamente a questão da territorialidade nas fraudes bancárias praticadas pela internet e demonstra que a jurisprudência tradicional, ao vincular a competência ao local da agência bancária, cria dificuldades concretas para a investigação e o julgamento. O autor mostra que, nas fraudes cibernéticas, é comum que vítima, criminoso e instituição financeira estejam em lugares distintos, muitas vezes em unidades federativas diferentes. Diante disso, sustenta que a lógica construída para delitos praticados no mundo físico não responde adequadamente à fluidez das operações virtuais, propondo que a competência seja definida a partir do domicílio ou residência da vítima, por ser critério mais compatível com a dinâmica desses crimes.

A contribuição de Otreira (2020) evidencia, de forma muito concreta, como a territorialidade se torna um dos pontos mais frágeis da aplicação do direito penal tradicional aos crimes digitais. Se o sistema clássico parte da ideia de um lugar relativamente determinado para a consumação da infração, o ambiente virtual rompe essa referência ao permitir que autor, vítima, dados e efeitos do crime estejam

pulverizados em espaços distintos. Por isso, a insistência em parâmetros estritamente físicos tende a dificultar a apuração e a retardar a resposta estatal. O problema não é apenas de competência formal, mas de efetividade investigativa, já que a definição inadequada do juízo pode comprometer o rápido acesso aos vestígios e a própria utilidade da prova digital.

Saad, Rossi e Partata (2024) concluem que a obtenção das provas digitais no processo penal demanda disciplina jurídica própria. Os autores demonstram que a prova digital possui características singulares, como imaterialidade, volatilidade, desprendimento do suporte físico, suscetibilidade de clonagem e necessidade de intermediação técnica. Tais particularidades fazem com que esses elementos sejam especialmente vulneráveis a alterações e questionamentos sobre autenticidade e confiabilidade. O estudo também indica que os meios de obtenção de dados digitais afetam direitos fundamentais relevantes, o que exige requisitos mínimos e procedimentos específicos para orientar a atuação judicial e investigativa.

A partir de Saad, Rossi e Partata (2024), percebe-se que a prova representa um dos pontos em que o direito penal tradicional mais claramente revela sua insuficiência diante dos crimes digitais. Isso ocorre porque os instrumentos probatórios clássicos foram pensados, em grande medida, para vestígios físicos, estáveis e perceptíveis, enquanto a prova digital é imaterial, facilmente copiável e altamente dependente de técnica especializada. Assim, a simples aplicação das regras tradicionais, sem adaptações, pode comprometer a cadeia de custódia, a confiabilidade dos dados e até a validade do material colhido. A discussão deixa evidente que a resposta penal adequada, no ambiente virtual, exige não apenas vontade repressiva, mas também precisão metodológica e fundamento normativo específico.

Fisberg (2025) examina a função *hash* como instrumento de garantia da integridade da prova digital e conclui que, embora essa técnica seja valiosa para verificar a integridade dos dados, ela não é infalível e depende de rigor técnico e conhecimento especializado. O autor demonstra que a prova digital inspira desafios próprios em razão de sua imaterialidade, volatilidade, fragilidade e dispersão, além de apontar divergências jurisprudenciais quanto ao tratamento do tema. O estudo mostra, assim, que a confiabilidade dos vestígios eletrônicos não pode ser presumida automaticamente, devendo resultar de procedimentos adequados de preservação e verificação.

A reflexão de Fisberg (2025) aprofunda o debate probatório ao demonstrar que, nos crimes digitais, não basta simplesmente ter acesso ao dado: é preciso garantir que esse dado permaneça íntegro, verificável e tecnicamente compreensível. Isso reforça a percepção de que a prova digital não se ajusta plenamente a uma lógica processual construída para objetos materiais. Se a materialidade do delito depende de registros eletrônicos frágeis e tecnicamente processados, a atuação penal precisa incorporar critérios mais especializados, sob pena de comprometer tanto a acusação quanto a defesa. Nesse ponto, os desafios da prova digital deixam de ser apenas operacionais e passam a atingir o próprio devido processo legal.

Ribeiro, Cordeiro e Fumach (2022) analisam o uso de malware como meio de obtenção de prova e concluem que, diante da legislação vigente, sua utilização não é admissível no ordenamento jurídico brasileiro. Os autores ressaltam que se trata de técnica altamente invasiva, capaz de acessar dados, funcionalidades e até sinais audiovisuais de dispositivos informáticos, o que impacta diretamente direitos fundamentais e garantias processuais. O artigo reconhece a eficiência potencial desse instrumento na investigação, mas afirma que sua adoção, sem disciplina legal específica, não encontra respaldo seguro no sistema jurídico atual.

Esse estudo mostra com clareza que a insuficiência legislativa não se manifesta apenas na falta de tipos penais, mas também na ausência de disciplina adequada para técnicas investigativas emergentes. Em outras palavras, o direito penal tradicional enfrenta dificuldades não só para descrever e enquadrar condutas digitais, mas também para definir até onde o Estado pode ir na busca de prova sem ultrapassar os limites constitucionais. Quando a criminalidade se sofisticou tecnologicamente, a investigação também passou a demandar instrumentos mais complexos; porém, sem base legal precisa, esses meios podem gerar nulidade e violação de garantias fundamentais. O problema, portanto, não é apenas de eficiência repressiva, mas de compatibilização entre investigação tecnológica e legalidade estrita.

Arigony, Botton e Arigony (2025) destacam a crescente utilização de provas digitais no processo penal e mostram que as ferramentas tecnológicas foram cruciais, no caso analisado, para coleta de evidências, identificação de autores e resolução do crime. Os autores apontam, contudo, que o uso dessas inovações também traz desafios éticos e jurídicos, reforçando a necessidade de modernização das práticas investigativas e de proteção de direitos fundamentais, como privacidade e presunção

de inocência. O estudo evidencia, assim, que a investigação criminal contemporânea depende cada vez mais de técnicas adaptadas ao ambiente digital.

A contribuição de Arigony, Botton e Arigony (2025) reforça que a insuficiência do modelo tradicional não significa incapacidade absoluta do sistema penal, mas necessidade de atualização de seus instrumentos. A investigação contemporânea já não pode prescindir de rastreamento digital, análise forense de dispositivos e exploração de dados eletrônicos; ao mesmo tempo, esses recursos exigem critérios jurídicos rigorosos para que não se convertam em meios arbitrários de intervenção. Isso mostra que o desafio central não está em abandonar o direito penal clássico, mas em repensar sua aplicação diante de um cenário em que a prova, a autoria e a materialidade se apresentam sob formas tecnicamente novas.

Maia e Costa (2023) sustentam que o combate aos crimes cibernéticos exige legislação dinâmica e ação coordenada entre governos e empresas. Os autores destacam que a segurança cibernética não é apenas questão técnica, mas tema de segurança pública e interesse coletivo, razão pela qual o poder público deve atuar de forma proativa na prevenção e punição dessas práticas. O estudo conclui que a rápida evolução da tecnologia impõe atualização constante do aparato normativo e institucional, pois a simples existência de leis não garante, por si só, resposta adequada a uma criminalidade em permanente mutação.

Os estudos de Maia e Costa (2023) permitem encerrar este tópico com uma percepção mais ampla: os desafios do direito penal tradicional frente aos crimes digitais não são episódicos, mas estruturais. A velocidade da transformação tecnológica, a transnacionalidade das condutas, a fragilidade dos vestígios eletrônicos e a sofisticação dos meios de ocultação revelam que o sistema penal clássico, sozinho, não consegue responder de forma integral a essa realidade. Por isso, a insuficiência legislativa deve ser compreendida não apenas como carência de normas, mas como necessidade de aperfeiçoamento contínuo da tipificação, da investigação, da cooperação institucional e do tratamento probatório, para que a repressão penal seja ao mesmo tempo eficaz e compatível com os direitos fundamentais.

Ao final, a análise dos autores permite concluir que a aplicação do direito penal tradicional aos crimes digitais encontra limites relevantes em cinco eixos centrais: a tipicidade, porque nem sempre os tipos clássicos acompanham a mutação das condutas virtuais; a prova, porque os vestígios digitais são imateriais, voláteis e tecnicamente dependentes de validação; a autoria, porque anonimização,

compartilhamento de IP e intermediação tecnológica dificultam a individualização do agente; a materialidade, porque sua demonstração depende de vestígios digitais frágeis, voláteis e tecnicamente processados; a territorialidade, porque o ciberespaço fragmenta a noção tradicional de lugar do crime; e a insuficiência legislativa, porque o avanço normativo, embora importante, ainda não eliminou lacunas na repressão e na investigação dessas condutas. Em síntese, os estudos convergem no sentido de que o enfrentamento da criminalidade digital exige releitura crítica das categorias penais clássicas e aperfeiçoamento contínuo dos instrumentos legislativos e processuais.

5 CONCLUSÃO

A pesquisa partiu da questão central de em que medida o direito penal tradicional, pensado para condutas materiais, territorialmente delimitadas e de autoria identificável, consegue responder de forma adequada aos crimes digitais praticados por meio ou contra sistemas informáticos.

Para isso, buscou-se contextualizar a criminalidade digital na sociedade da informação, conceituar e classificar os crimes digitais, examinar os princípios e a estrutura clássica do direito penal e identificar os principais entraves à sua aplicação, além de mapear a evolução legislativa brasileira sobre o tema.

Esses objetivos foram atingidos ao se evidenciar, de maneira articulada, os pontos de tensão entre a realidade tecnológica contemporânea e o modelo penal clássico. Os resultados mostraram que os crimes digitais são expressão de um contexto técnico-social marcado pela centralidade da informação, pela sociedade em rede e pela virtualização das relações sociais e jurídicas.

A doutrina já oferece uma conceituação funcional e uma tipologia relativamente consolidada, distinguindo crimes próprios, impróprios e híbridos, bem como identificando espécies recorrentes no cenário brasileiro, como invasão de dispositivos, fraudes eletrônicas, crimes contra a honra em redes sociais e violações de dados pessoais.

O estudo contribui ao sistematizar o diálogo entre sociedade da informação, criminalidade digital e dogmática penal, apontando que o problema não se resume à ausência de leis, mas atinge a própria forma como o sistema penal foi estruturado. Já para a prática jurídica, os achados reforçam a necessidade de que operadores do direito reconheçam os limites do modelo tradicional diante da criminalidade digital e atuem com maior cuidado em temas como prova eletrônica, definição de competência e proteção de direitos fundamentais em ambiente virtual.

Entre as limitações, destaca-se o caráter exclusivamente bibliográfico e documental da pesquisa, sem investigação empírica sobre casos concretos ou sobre a percepção de integrantes do sistema de justiça, bem como a constante mutação tecnológica, que pode tornar algumas análises parcialmente superadas em pouco tempo.

Essas restrições, porém, indicam caminhos para estudos futuros, como pesquisas empíricas sobre a atuação de delegacias especializadas, ministério público

e poder judiciário, análises comparadas entre ordenamentos jurídicos e investigações específicas sobre prova digital, cooperação internacional e responsabilidade penal em cenários de anonimato e automação.

A necessidade de atualização permanente da dogmática e da legislação sugere que a compatibilidade entre direito penal tradicional e criminalidade digital tende a permanecer como um dos desafios centrais do sistema penal na sociedade da informação.

REFERÊNCIAS

ALBANO, Ana Laura. **Contratos e assinaturas digitais nas transações imobiliárias**: uma análise da validade jurídica na era digital. 2023. Disponível em: <<https://educapes.capes.gov.br/handle/11449/253471>>. Acesso em: 12 set. 2025.

ÂNGELO, Marcel Alves Di. **Democracia, desinformação e direito**: os desafios do regramento do debate público na internet em perspectiva sociojurídica. 2025. Disponível em: <https://bdtd.ibict.br/vufind/Record/UCB_de6f55b8d51c0890749328dfc8914f5f>. Acesso em: 12 set. 2025.

ARAÚJO FILHO, João Souza. **A evolução das normas do direito digital brasileiro**: da indústria de informática à constitucionalização da proteção de dados. 2025. Disponível em: <<https://repositorio.ufu.br/handle/123456789/46453>>. Acesso em: 30 set. 2025.

ARAÚJO, Tuiyane Filgueiras Mendes. **Os desafios do Direito Penal na proteção das crianças e adolescentes na era digital**: uma análise da repressão dos crimes cibernéticos à luz da Lei 14.811/24. Trabalho de Conclusão de Curso (Bacharelado em Direito) - Faculdade Nacional de Direito, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2024. Disponível em: <<https://pantheon.ufrj.br/handle/11422/25324>>. Acesso em: 18 out. 2025.

ARIGONY, Marcelo Mendes; BOTTON, Letícia Thomasi Jahnke; ARIGONY, Ana Luiza Ortiz. Persecução penal digital: a prova na era da informação. **Direito & TI**, [S. l.], v. 1, n. 20, p. 1-22, 2025. Disponível em: <https://direitoeti.com.br/direitoeti/article/view/268>. DOI: <https://doi.org/10.63451/dti.v1i20.268>. Acesso em: 5 abr. 2026.

ASSUNÇÃO, Linara Oeiras. Notas Sobre A Política Brasileira De Ciência, Tecnologia E Inovação: em defesa de uma elaboração legislativa de qualidade. **LEGÍSTICA**, p. 169, 2019. Disponível em: <<https://www.escavador.com/sobre/6401315/linara-oeiras-assuncao>>. Acesso em: 12 set. 2025.

AVELINO, Laryssa Ribeiro. **Responsabilidade civil dos agentes de tratamento em casos de violação à proteção de dados pessoais**: uma análise dos sistemas brasileiro e europeu. 2024. Disponível em: <<https://repositorio.idp.edu.br/handle/123456789/5165>>. Acesso em: 07 ago. 2025.

BAPTISTA JUNIOR, José Roberto. **POR UM DIREITO PENAL EFICAZ: UMA CONSTRUÇÃO CRÍTICA PARA ALÉM DO EFICIENTISMO**. 2020. Disponível em: <<https://www.escavador.com/sobre/6360351/roberto-da-freiria-estevao>>. Acesso em: 12 dez. 2025.

BARROS, Bruno Pereira. **Crimes cibernéticos**: dificuldade para obter indícios de autoria e materialidade. 2023. Disponível em: <<https://www.escavador.com/sobre/454897/gil-cesar-costa-de-paula>>. Acesso em: 12 out. 2025.

BESTETTI, Gabriel Guazzelli. **Os desafios do Direito no combate aos crimes virtuais**. 2023. Disponível em: <<https://lume.ufrgs.br/handle/10183/276738?show=full>>. Acesso em: 09 dez. 2025.

BICALHO, Camila Fernandes. **Crimes patrimoniais na era digital**: contribuições da teoria das atividades rotineiras. 2024. Disponível em: <<https://repositorio.ufmg.br/handle/1843/80146>>. Acesso em: 10 mar. 2025.

BODIN, Celina. Redes sociais virtuais: privacidade e responsabilidade civil. Análise a partir do Marco Civil da Internet. **Pensar-Revista de Ciências Jurídicas**, 2017. Disponível em: <<https://ojs.unifor.br/rpen/article/view/6272>>. Acesso em: 12 set. 2025.

BRASIL. **Decreto-Lei n.º 2.848, de 7 de dezembro de 1940**. Código Penal. Brasília, DF: Presidência da República, 1940. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acesso em: 11 dez. 2025.

BRASIL. **Lei n.º 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 12 dez. 2025.

BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm>. Acesso em: 19 jun. 2025.

BRASIL. **Lei n.º 14.155, de 27 de maio de 2021**. Altera o Decreto-Lei n.º 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet. Brasília, DF: Presidência da República, 2021. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm>. Acesso em: 19 jun. 2025.

BRASIL. **Lei n.º 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF: Presidência da República, 1990. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm>. Acesso em: 04 dez. 2025.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Marco Civil da Internet. Diário Oficial da União, Brasília, DF, 24 abr. 2014. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 19 jun. 2025.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 25 nov. 2025.

BRASILEIRO, Fellipe Sá. **Resiliência informacional**: modelo baseado em práticas informacionais colaborativas em redes sociais virtuais. 2017. Disponível em:

<https://repositorio.ufpb.br/jspui/handle/tede/9710?locale=pt_BR>. Acesso em: 30 out. 2025.

BROCHADO, Isabelle Pinto da Silva. **Investigação de crimes cibernéticos nas Polícias Cíveis do Brasil**: contribuição da gestão do conhecimento. 2025. Disponível em: <<https://repositorio.ufsc.br/handle/123456789/265749>>. Acesso em: 17 nov. 2025.

CAMARGO, Rodrigo Oliveira de. **Tratamento de dados, persecução penal e garantia do direito de defesa**. 2022. Disponível em: <<https://tede2.pucrs.br/tede2/handle/tede/10605>>. Acesso em: 20 out. 2025.

CANESTRARO, Anna Carolina; JANUÁRIO, Túlio Felipe Xavier. Responsabilidade penal da pessoa coletiva e princípio da culpabilidade: análise crítica do modelo português. **Revista da Faculdade de Direito da UFRGS**, n. 39, 2018. Disponível em: <<https://seer.ufrgs.br/index.php/revfacdir/article/view/77092>>. Acesso em: 07 nov. 2025.

CARVALHO, Pedro Augusto Mutton de. **Camadas e estrutura da internet e regulação estatal**: estratégias para efetivação internacional dos direitos humanos em ambiente democrático. 2024. Disponível em: <<https://repositorio.sis.puc-campinas.edu.br/handle/123456789/14932/browse?type=author&value=Carvalho%C3%A7PedroAugustoMuttonde>>. Acesso em: 17 set. 2025.

CASTRO, Pablo Domingues Ferreira de. **Justa causa material no direito penal**: necessário filtro de responsabilização criminal como teoria legitimadora num processo acusatório democrático. 2023. Disponível em: <<https://www.escavador.com/sobre/910554/pablo-domingues-ferreira-de-castro>>. Acesso em: 04 nov. 2025.

CERVO, Amado Luiz; BERVIAN, Pedro Alcino. **Metodologia Científica**. 5. ed. São Paulo: Prentice Hall, 2002.

COELHO, Edihermes Marques. Prescrição penal como limite ao poder-dever punitivo estatal. **Revista Jurídica UNICURITIBA**, Curitiba, v. 3, n. 60, p. 339-360, 2020. Disponível em: <<https://revista.unicuritiba.edu.br/index.php/RevJur/article/view/4185>>. Acesso em: 22 ago. 2025.

CORDEIRO, Flávio Vinícius Alves; MORAIS, Rafael Matos de Freitas. PROVA DIGITAL: ESTUDO SOBRE A DECISÃO DO SUPERIOR TRIBUNAL DE JUSTIÇA QUE RECONHECEU A NULIDADE DE PROVA OBTIDA DO WHATSAPP WEB. **Revista Contemporânea**, v. 4, n. 4, p. e3846-e3846, 2024. Disponível em: <<https://ojs.revistacontemporanea.com/ojs/index.php/home/article/view/3846>>. Acesso em: 17 nov. 2025.

CORRÊA, Fernando Gabriel; MARQUES, Angelica Alves da Cunha. Princípio da territorialidade: trajetórias e definições. **ÁGORA: Arquivologia em debate**, v. 26, n. 52, p. 05-29, 2016. Disponível em: <<https://agora.emnuvens.com.br/ra/article/view/582>>. Acesso em: 17 jul. 2025.

CORTEZ, Danielle Martins da Câmara. **O direito administrativo sancionador e o princípio da culpabilidade no âmbito dos Tribunais de Contas**. 2017. Disponível em: <<https://repositorio.ufrn.br/items/08dddc92-70fd-45f4-876a-ea1a84bcd2ad>>. Acesso em: 27 jul. 2025.

COUTO, Brunno Pereira Soares; FERREIRA, Isadora Santiago dos Santos. O crime de perseguição no Brasil: análise dogmática e reflexão sobre o fato típico e ilícito. **Rev. Severa Verum Gaudium**, v. 7, n. 1, 2022. Disponível em: <<https://seer.ufrgs.br/index.php/resseveraverumgaudium/article/view/124818>>. Acesso em: 17 nov. 2025.

DAVID, Décio Franco. Considerações sobre as garantias do princípio da culpabilidade no Direito Penal Econômico. **Revista do Instituto Brasileiro de Direito Penal Econômico**. Florianópolis: Empório do Direito, v. 1, p. 157-188, 2016. Disponível em: <<https://ibdpe.com.br/publicacoes/revista-do-ibdpe-volume-1/>>. Acesso em: 10 mai. 2025. Acesso em: 17 nov. 2025.

DEOLINDO, Emylliane. **Populismo penal e mídia: uma análise dos impactos do discurso punitivo na política criminal contemporânea**. 2025. Tese de Doutorado. Disponível em: <<https://repositorio.ulisboa.pt/entities/publication/4584471d-24e6-4800-9199-2f275151cfc0>>. Acesso em: 18 ago. 2025.

DIAS, Donaldo de Souza; SILVA, Mônica Ferreira. **Como escrever uma monografia: manual de elaboração com exemplos e exercícios**. São Paulo: Altas, 2010.

EISELE, Andreas. Direito penal. Teoria do delito, **JusPODIVM**, Salvador, 2018. Disponível em: <<https://bdjur.stj.jus.br/entities/publication/44cf9f34-58c5-46cb-b731-1dce6896e388/full>>. Acesso em: 27 jul. 2025.

FARIAS, Karina da Hora. **Impactos dos crimes cibernéticos e os riscos da inteligência artificial: os pilares do direito na proteção dos dados sensíveis**. 2022. Disponível em: <<https://repositorio.ufba.br/xmlui/handle/ri/36911?locale-attribute=en&show=full>>. Acesso em: 15 nov. 2025.

FÉRES, Rodrigo Pinheiro. **Uso de informações armazenadas em meio digital no processo penal**. 2021. Disponível em: <<https://repositorio.idp.edu.br/handle/123456789/4754>>. Acesso em: 11 jan. 2026.

FERNANDES, Marquêsia Pereira. **Crimes digitais na era do metaverso no Brasil**. 2022. Disponível em: <<https://repositorio.pucgoias.edu.br/jspui/bitstream/123456789/4923/1/MARQU%C3%89SIA%20PEREIRA%20FERNANDES.pdf>>. Acesso em: 15 nov. 2025.

FERREIRA FILHO, Agnaldo Adriano; TORRE, Leonardo Guimarães. Crimes digitais e suas implicações legais. **Revista Eletrônica Acervo Científico (REASE)**, 2024. Disponível em: <<https://periodicorease.pro.br/rease/issue/view/62>>. Acesso em: 05 mar. 2025.

FERREIRA JUNIOR, Edinaldo Inocêncio. Conceito analítico de crime: um estudo dogmático de seus elementos essenciais à caracterização do fato punível. **Revista Contemporânea**, v. 3, n. 6, p. 6034-6050, 2023. Disponível em: <<https://www.resear>

chgate.net/publication/371767082_conceito_analitico_de_crime_um_estudo_dogmatico_de_seus_elementos_essenciais_a_caracterizacao_do_fato_punivel>. Acesso em: 12 set. 2025.

FIGUEIREDO, Gabriella Pessoa de. **Crítérios jurídicos para uma jurisdição eficiente no metaverso**: desafios e perspectivas. 2025. Trabalho de Conclusão de Curso. Universidade Federal do Rio Grande do Norte. Disponível em: <<https://repositorio.ufrn.br/items/1e7257cf-6428-4a7c-82b5-3592e7ddfc0a>>. Acesso em: 20 nov. 2025.

FILIPPO, Thiago Baldani Gomes de. **Proporcionalidade legislativa penal**: propostas para o aperfeiçoamento dos tipos e para o equilíbrio entre as sanções do direito penal brasileiro. 2020. Tese de Doutorado. Universidade de São Paulo. Disponível em: <https://bdtd.ibict.br/vufind/Record/USP_a1c72a2ffdc5a387b41814249a50aaea/Deta>. Acesso em: 02 nov. 2025.

FISBERG, Yuri. Função 'hash' e a integridade da prova digital. **Revista Brasileira de Direito Processual Penal**, Porto Alegre, v. 11, n. 3, e1227, set./dez. 2025. Disponível em: <https://revista.ibraspp.com.br/RBDPP/article/view/1227>. DOI: <https://doi.org/10.22197/rbdpp.v11i3.1227>. Acesso em: 5 abr. 2026.

FLORES, Maria Eduarda Rodrigues. **Os Crimes Cibernéticos**: Desafios e Implicações Legais na Era Digital. 2025. Disponível em: <<https://repositorio.pucgoias.edu.br/jspui/handle/123456789/10330>>. Acesso em: 06 mar. 2026.

FLORES, Maria Eduarda Rodrigues. **Os Crimes Cibernéticos**: Desafios e Implicações Legais na Era Digital. 2025. Disponível em: <<https://repositorio.pucgoias.edu.br/jspui/handle/123456789/10330>>. Acesso em: 5 mar. 2026.

GARMES, Felipe Maiolo. **Bem jurídico penal**: proteção e limites à luz da constitucionalização do direito penal. 2025. Disponível em: <<https://repositorio.pucsp.br/jspui/handle/handle/44191?mode=full>>. Acesso em: 18 jan. 2026.

GIL, Antônio Carlos. **Métodos e Técnicas de Pesquisa Social**. 5. ed. São Paulo: Atlas, 1999.

GIORGI JUNIOR, Romulo Ponticelli. **Jurisdição constitucional e código de processo civil**: sincronia, racionalidade, interpretação e segurança jurídica. 2016. Disponível em: <<https://lume.ufrgs.br/handle/10183/148766>>. Acesso em: 18 jan. 2026.

GOIÁS (Estado). Poder Judiciário. Comarca de Rio Verde. 2º Juizado Especial Cível e Criminal. **Processo n.º 5868405-47.2025.8.09.0137**. Requerente: Mara Eliza José de Matos Silva Mendes. Requeridas: Facebook Serviços Online do Brasil Ltda. e Telefônica Brasil S.A. Sentença. Rio Verde, 2026. Disponível em: <<https://www.jusbrasil.com.br/jurisprudencia/tj-go/5689375175>>. Acesso em: 12 set. 2025.

GOMES, Julio Cesar Lôbo; MEDRADO, Lucas Cavalcante; GAMA, Giliarde Benavinto Albuquerque CVR N. **CRIMES CIBERNÉTICOS**: desafios jurídicos no processo e julgamento de infrações penais virtuais cometidas por agentes

estrangeiros contra vítimas brasileiras. **Revista JRG de Estudos Acadêmicos**, v. 7, n. 15, p. e151563-e151563, 2024. Disponível em: <<https://revistajrg.com/index.php/jrg/article/view/1563>>. Acesso em: 14 jul. 2025.

GOMES, Sílvia; CRUZ, Rui Vieira. Futureal: crime e tecnologias convergentes em Psycho-Pass. Configurações. **Revista Ciências Sociais**, n. 24, p. 96-121, 2019. Disponível em: <<https://journals.openedition.org/configuracoes/7802>>. Acesso em: 12 set. 2025.

GUINEZI, Daniel Torres. **Mensurando interações**: modelos de rede e aplicações à pesquisa em comunicação. 2020. Tese de Doutorado. Universidade de São Paulo. Disponível em: <https://www.oasisbr.ibict.br/vufind/Record/USP_20eaba5831de6e4ebd259c57d38885aa?lng=pt-br>. Acesso em: 13 dez. 2025.

HAMMERSCHMIDT, Karina Silveira; DAVID, Décio Franco. RESPONSABILIDADE PENAL DA PESSOA COLETIVA E O PRINCÍPIO DA CULPABILIDADE NOS CRIMES INFORMÁTICOS EM REDES SOCIAIS. **Caderno PAIC**, 2023. Disponível em: <<https://cadernopaic.fae.emnuvens.com.br/cadernopaic/article/view/559>>. Acesso em: 27 jul. 2025.

HENRIQUES, Thiago Alves; GONÇALVES, Samuel Martins. CRIMES DIGITAIS: análise sobre o Estelionato virtual. **Revista Eletrônica de Ciências Jurídicas**, v. 14, n. 1, 2024. Disponível em: <<https://revista.fadipa.br/index.php/cjuridicas/article/view/576>>. Acesso em: 12 set. 2025.

JURKEVICZ, Maristela Romagnole de Araujo. **Ressignificação dos processos comunicacionais a partir da utilização das tecnologias da informação e comunicação**: um repensar sobre o ensino de relações públicas e a formação profissional. 2017. Disponível em: <https://www.oasisbr.ibict.br/vufind/Record/RCAP_1df4d663d59b7440b46c0def1fa761c6>. Acesso em: 26 out. 2025.

JUSTINIANO, Nara Fernanda. **Terminologia e tecnologia**: um estudo de termos de crimes cibernéticos [em linha]. 2024. Disponível em: <<https://repositorio.unb.br/handle/10482/22977>>. Acesso em: 26 out. 2025.

LIMA, Isabel Muniz. **Modos de interação em contexto digital**. 2022. Tese de Doutorado. Universidade NOVA de Lisboa (Portugal). Disponível em: <<https://repositorio.ufc.br/handle/riufc/64516>>. Acesso em: 17 out. 2025.

LIRA, Cristiane da Silva Coimbra. **A tecnologia digital como ferramenta para inovação social, no contexto de uma organização para impacto social**. Universidade Federal de Santa Catarina. Programa de Pós-Graduação em Engenharia e Gestão do Conhecimento. Florianópolis, 2018. Disponível em: <<https://ppgegc.paginas.ufsc.br/2017/12/21/21-02-2018-dissertacao-cristiane-da-silva-coimbra-lira/>>. Acesso em: 26 set. 2025.

LUSTOSA, Thalita Furtado Mascarenhas. **A flexibilização das relações de trabalho na era das novas tecnologias**: reflexos econômicos e desafios jurídicos para a proteção dos trabalhadores. 2025. Disponível em: <[https://bdtd.ibict.br/vufind/search/results?bool%5B%5D=AND&filter%5B%5D=author_facet%3A%22Lustosa%](https://bdtd.ibict.br/vufind/search/results?bool%5B%5D=AND&filter%5B%5D=author_facet%3A%22Lustosa%22)>

2C+Thalita+Furtado+Mascarenhas%22&filter%5B%5D=dc.subject.eng.fl_str_mv%3A%22Technologies%22&filter%5B%5D=dc.subject.por.fl_str_mv%3A%22Tecnologias%22&join=AND&lookfor0%5B%5D=&sort=year&type0%5B%5D=AllFields>. Acesso em: 26 out. 2025.

MACHADO, Vitor Taveira. **A evolução legislativa dos crimes cibernéticos no ordenamento jurídico brasileiro**. 2023. Disponível em: <https://tede.pucsp.br/handle/handle/18763/simple-search?etal=0&filter_field_1=access&filter_type_1>equals&filter_value_1=Acesso+Aberto&filtername=advisor&filterquery=Souza%2C+Motauri+Ciocchetti+de&filtertype>equals&order=desc&query=&rpp=10&sort_by=score>. Acesso em: 14 out. 2025.

MAIA, Karolline Barbosa; COSTA, Cezar Henrique Ferreira. Crimes cibernéticos. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, [S. l.], v. 9, n. 10, p. 109-126, 2023. Disponível em: <https://periodicorease.pro.br/rease/article/view/11580>. DOI: <https://doi.org/10.51891/rease.v9i10.11580>. Acesso em: 5 abr. 2026.

MAIA, Teymisso Sebastian Fernandes. **Análise dos mecanismos de combate aos crimes cibernéticos no sistema penal brasileiro**. 2017. Disponível em: <<https://pt.scribd.com/document/607603452/2017-tcc-tsmaia>>. Acesso em: 26 out. 2025.

MAROUF, Giovanna Thaís dos Santos. **Crimes cibernéticos na era do consumidor digital e a atuação do compliance na privacidade de dados pessoais**. 2024. Disponível em: <<https://repositorio.pucsp.br/jspui/handle/handle/42762>>. Acesso em: 26 out. 2025.

MARTINS, Ana Letícia de Andrade. **Condutas ilícitas na internet e proteção penal**. 2024. Disponível em: <<https://repositorio.uema.br/handle/123456789/3347>>. Acesso em: 13 out. 2025.

MARTINS, João Júlio Ribeiro. **Os Equipamentos da Era Digital e a sua influência no Combate ao Crime Organizado**. 2023. Disponível em: <<https://comum.rcaap.pt/entities/publication/7d9aeab6-f2f7-4ba7-90d2-175d186f56a2>>. Acesso em: 26 dez. 2025.

MEDEIROS, Jackson Tavares da Silva; NELSON, Rocco Antonio Rangel Rosso. A constitucionalidade do poder normativo das agências reguladoras na ótica do redimensionamento do princípio da legalidade. **Revista de Direito Administrativo**, v. 271, p. 109-141, 2016. Disponível em: <<https://periodicos.fgv.br/rda/article/view/60763>>. Acesso em: 13 jul. 2025.

MELLO, Pablo da Silva de. **CRIMES VIRTUAIS E A LEGISLAÇÃO PENAL**. 2022. Disponível em: <<https://repositorio.pgsscogna.com.br/bitstream/123456789/66234/1/Pablo%2Bda%2BSilva%2BMello.pdf>>. Acesso em: 27 jul. 2025.

MELO, Anne Carollyne Vilanova de. **Evidências do expansionismo penal na esteira da regulamentação das novas tecnologias de comunicação**. 2024. Disponível em: <<https://ri.ufs.br/handle/riufs/20407?mode=full>>. Acesso em: 26 out. 2025.

MONTEIRO, Jean Carlos da Silva; FAÇANHA, Luciano da Silva. As TIC no centro da (re)configuração social do século XXI. 2025. Disponível em: <<https://periodicos.ufmg.br/index.php/textolivre/article/view/56501>>. Acesso em: 26 out. 2025.

MONTEL, Izadora Fonseca; PAIVA, Jaqueline de Kassia Ribeiro de. Crimes cibernéticos: panorama legislativo. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, [S. l.], v. 10, n. 11, p. 4495-4523, 2024. Disponível em: <https://periodicorease.pro.br/rease/article/view/17070>. DOI: <https://doi.org/10.51891/rease.v10i11.17070>. Acesso em: 5 abr. 2026.

MORAES, Andrei Sodre. **A função preventiva da lei penal**. 2022. Disponível em: <https://www.oasisbr.ibict.br/vufind/Record/Krot_b8629b4107db4f674dd202ec424354f6>. Acesso em: 15 mai. 2025.

MORAIS, Maria Luiza Sampaio. **A EVOLUÇÃO DOS CRIMES CIBERNÉTICOS: DESAFIOS DA INVESTIGAÇÃO DIGITAL E A ADAPTAÇÃO DA LEGISLAÇÃO FRENTE AO AVANÇO TECNOLÓGICO**. 2025. Disponível em: <<https://repositorio.pucgoias.edu.br/jspui/handle/123456789/10259>>. Acesso em: 26 mar. 2025.

NUNES, Isaura Manuela Pimentel. **Inclusão digital como direito fundamental na sociedade da informação: tecnologia, cidadania, envelhecimento e novas formas de exclusão**. 2025. Disponível em: <<https://ri.ucsal.br/collections/a246eba1-a852-4c56-b1db-84ad9c189fea>>. Acesso em: 15 out. 2025.

NUNES, Lucyene Lopes da Silva Todesco. Educação em rede: tendências tecnológicas e pedagógicas na sociedade em rede. **Em Rede-Revista de Educação a Distância**, v. 3, n. 2, p. 197-212, 2016. Disponível em: <<https://www.auniredede.org.br/revista/index.php/emrede/article/view/116>>. Acesso em: 12 set. 2025.

OLIVEIRA, Daniel Calegar. **Direitos fundamentais e a era digital: Limites no exercício dos direitos fundamentais e sua aplicação na internet**. Repositório de Trabalhos de Conclusão de Curso, 2023. Disponível em: <<https://pensaracademico.unifacig.edu.br/index.php/repositoriottcc/article/view/4164>>. Acesso em: 26 out. 2025.

OLIVEIRA, Dyéssica Thaís Santos; CUNHA, Aline Sales da; SILVA, Hernando Fernandes. RESPONSABILIDADE PENAL NO ANONIMATO DIGITAL: OS DESAFIOS DE INVESTIGAÇÕES E PROVA À LUZ DA LEI 14.811/2024. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, v. 11, n. 5, p. 2651-2672, 2025. Disponível em: <https://www.researchgate.net/publication/391725291_responsabilidade_penal_no_anonimato_digital_os_desafios_de_investigacoes_e_prova_a_luz_da_lei_148112024criminal_liability_in_digital_anonymity_challenges_of_investigation_and_evidence_under_law_no_148>. Acesso em: 26 out. 2025.

OLIVEIRA, Geovana Xavier de. **Crimes cibernéticos: direito digital e os novos paradigmas da investigação criminal**. 2022. Disponível em: <https://repositorio.pucgoias.edu.br/jspui/browse?etal=-1&null=&offset=2468&order=ASC&rpp=20&sort_by=1&type=title>. Acesso em: 13 dez. 2025.

OLIVEIRA, Giovanna Aleixo Gonçalves; ÁVILA, Gustavo Noronha de. Deep fake, direitos da personalidade e o direito penal: uma análise dos impactos tecnológicos na

era digital. **Revista Eletrônica do Curso de Direito da UFSM**, p. e85239-e85239, 2024. Disponível em: <<https://periodicos.ufsm.br/revistadireito/article/view/85239>>. Acesso em: 26 out. 2025.

OTREIRA, Leonardo. **A competência territorial nas fraudes bancárias praticadas pela internet**. Boletim Científico Escola Superior do Ministério Público da União, Brasília, a. 19, n. 55, p. 277-292, jan./dez. 2020. Disponível em: <https://escola.mpu.mp.br/publicacoesscientificas/index.php/boletim/article/view/575>. DOI: <https://doi.org/10.63601/bcesmpu.2020.n55.277-292>. Acesso em: 5 abr. 2026.

PEREIRA, João Victor Gonçalves. **Metaverso e as novas tecnologias digitais: um estudo sobre o novo modelo de realidade virtual e as mudanças paradigmáticas das relações públicas**. 2022. Disponível em: <https://www.repositorio.ufal.br/bitstream/123456789/13463/1/Metaverso%20e%20as%20novas%20tecnologias%20digitais_um%20estudo%20sobre%20o%20novo%20modelo%20de%20realidade%20virtual%20e%20as%20mudan%C3%A7as%20paradigm%C3%A1ticas%20da%20rela%C3%A7%C3%B5es%20p%C3%ABlicas.pdf>. Acesso em: 5 abr. 2026.

PEREIRA, Vitória Costa. **EXECUÇÃO PENAL DOS CRIMES CONTRA O PATRIMÔNIO: a pena de multa à luz da criminologia crítica do conflito**. 2024. Disponível em: <<https://repositorio.ufpb.br/jspui/handle/123456789/34207>>. Acesso em: 18 jan. 2026.

PLENS, Leonardo Mariuzzo. **Tipicidade penal e o princípio da insignificância**. 2025. Disponível em: <<https://repositorio.ulisboa.pt/entities/publication/28968cdf-35a6-47c8-a00f-226a30b1b6c7>>. Acesso em: 18 jan. 2026.

PRESTES, Felipe Pinheiro. **OS DELITOS INFORMÁTICOS E A JURISDIÇÃO CRIMINAL NO CIBERESPAÇO. DIREITO E TECNOLOGIA**, p. 47. 2020. Disponível em: <<https://periodicos.unesc.net/ojs/index.php/AnaisDirH/article/view/9381>>. Acesso em: 22 jan. 2026.

QUEIROZ, Liv Ferreira Augusto Severo. Os crimes cibernéticos no ordenamento jurídico brasileiro: investigação criminal e desafios. **Revista do CNMP**, Brasília, n. 12, p. 417-448, 2024. Disponível em: <https://ojs.cnmp.mp.br/index.php/revistacnmp/article/view/707>. DOI: <https://doi.org/10.36662/revistadocnmp.i12.707>. Acesso em: 5 abr. 2026.

RESENDE, Augusto César Leite de; MOLINARO, Carlos Alberto. A interamericanização do direito administrativo sancionador brasileiro: reflexões sobre o princípio da tipicidade da infração disciplinar a partir do diálogo judicial internacional. **A&C-Revista de Direito Administrativo & Constitucional**, v. 19, n. 76, p. 153-173, 2019. Disponível em: <<https://dspace.almg.gov.br/handle/11037/38022?locale=en>>. Acesso em: 27 jul. 2025.

RIBEIRO, Gustavo Alves Magalhães; CORDEIRO, Pedro Ivo Rodrigues Velloso; FUMACH, Débora Moretti. O malware como meio de obtenção de prova e a sua implementação no ordenamento jurídico brasileiro. **Revista Brasileira de Direito Processual Penal**, Porto Alegre, v. 8, n. 3, p. 1463-1500, set./dez. 2022. Disponível

em: <https://revista.ibraspp.com.br/RBDPP/article/view/723>. DOI: <https://doi.org/10.22197/rbdpp.v8i3.723>. Acesso em: 5 abr. 2026.

ROCHA, Sergio André. A origem do princípio da tipicidade no direito tributário brasileiro. **Revista Direito Tributário Atual**, n. 50, p. 399-430, 2022. Disponível em: <<https://revista.ibdt.org.br/index.php/RDTA/article/view/2137>>. Acesso em: 18 jan. 2026.

ROCHA, Veronica Alkmim. AS (IN) EFICIÊNCIAS COMPROBATÓRIAS DA LEGISLAÇÃO BRASILEIRA E OS DESAFIOS DA PERSECUÇÃO PENAL NOS CRIMES DE INVASÃO DE DISPOSITIVOS INFORMÁTICOS: UMA ANÁLISE À LUZ DAS LEIS 12.737/2012 E 14.155/2021. **LUMEN ET VIRTUS**, v. 16, n. 51, p. e7041-e7041, 2025. Disponível em: <<https://periodicos.newsciencepubl.com/LEV/citationstylelanguage/get/turabian-fullnote-bibliography?issuelid=99&publicationId=7042&submissionId=7041>>. Acesso em: 18 mai. 2026.

RODRIGUES, Susana Almeida. **Serviço social frente às tecnologias digitais da informação e comunicação: uma análise a partir de dissertações e teses (1990-2021)**. 2022. Disponível em: <<https://ri.ufs.br/handle/riufs/17544?locale=en>>. Acesso em: 18 jan. 2026.

SAAD, Marta; ROSSI, Helena Costa; PARTATA, Pedro Henrique. A obtenção das provas digitais no processo penal demanda uma disciplina jurídica própria? Uma análise do conceito, das características e das peculiaridades das provas digitais. **Revista Brasileira de Direito Processual Penal**, Porto Alegre, v. 10, n. 3, e1071, set./dez. 2024. Disponível em: <https://revista.ibraspp.com.br/RBDPP/article/view/1071>. DOI: <https://doi.org/10.22197/rbdpp.v10i3.1071>. Acesso em: 5 abr. 2026.

SALIM, Alexandre; AZEVEDO, Marcelo André de. **Direito Penal**. Salvador: Juspodivm, 2019.

SANTOS, Carlos Mickael da Silva. **Crimes informáticos: uma análise sob a perspectiva do direito penal e processual penal**. 2021. Disponível em: <<https://repositorio.unisc.br/jspui/handle/11624/3271>>. Acesso em: 25 jan. 2026.

SANTOS, Pedro Henrique Costa; FERREIRA, Camyla de Sousa Franco. Princípio da legalidade penal: uma manobra de proteção e à dignidade humana. **Revista Foco**, v. 17, n. 6, p. e5348-e5348, 2024. Disponível em: <https://www.researchgate.net/publication/381621784_principio_da_legalidade_penal_uma_manobra_de_protecao_e_a_dignidade_humana>. Acesso em: 18 jan. 2026.

SANTOS, Rogério Gomes dos; OLIVEIRA, Jocirley de. OS DESAFIOS E AS PERSPECTIVAS DO DIREITO NA ERA DIGITAL: ADAPTAÇÃO NORMATIVA E TECNOLÓGICA PARA A PROTEÇÃO DOS DIREITOS E GARANTIAS INDIVIDUAIS NA SOCIEDADE DIGITAL. **Facit Business and Technology Journal**, v. 2, n. 63, 2025. Disponível em: <<https://revistas.faculdefacit.edu.br/index.php/JNT/article/view/File/3594/2421>>. Acesso em: 15 nov. 2025.

SANTOS, Samuel Huhn Saldanha; DOMINGOS, Ana Luiza Gouveia; SANTOS, Yan Carlos Maria dos Maria dos; FIGUEIREDO, Cristiane Xavier. TRATAMENTO

JURÍDICO DOS CRIMES COMETIDOS EM AMBIENTE VIRTUAL. **Revista Jurídica do Nordeste Mineiro**, v. 4, n. 1, 2024. DOI: 10.61164/rjnm.v4i1.2296. Disponível em: <https://jrnrm.ojsbr.com/juridica/article/view/2296>. Acesso em: 6 ago. 2025.

SANTOS, Yan Carlos Maria dos Maria dos; BOTELHO, Daniela Garcia. A influência das novas tecnologias no direito penal—desafios e perspectivas. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, v. 9, n. 11, p. 2713-2726, 2023. Disponível em: <<https://periodicorease.pro.br/rease/article/view/12347>>. Acesso em: 12 dez. 2025.

SEVERINO, Antônio Joaquim. **Metodologia do trabalho científico**. 23. ed. ver. e atual. São Paulo: Cortez, 2007.

SILVA, Ana Laura Rossi. **Cibercrimes**: uma análise sob a perspectiva da aplicação do Direito Internacional. 2019. Disponível em: <<https://repositorio.ufu.br/handle/123456789/28413>>. Acesso em: 12 dez. 2025.

SILVA, Iris Nathalia da. **Liberdade de Expressão e Responsabilidade Civil nas Plataformas de Redes Sociais**: As Insuficiências do Marco Civil da Internet. 2024. Disponível em: <<https://repositorio.ufsc.br/handle/123456789/262804?locale-attribute=es>>. Acesso em: 28 dez. 2025.

SILVA, Ruan Martins da. **CRIMES VIRTUAIS**: uma abordagem da conduta criminosa por meio da internet. 2022. Disponível em: <<https://www.monografias.ufma.br/jspui/handle/123456789/8698?mode=full>>. Acesso em: 01 dez. 2025.

SOARES, Igor Azerêdo. **Celeridade e Eficácia da Investigação Policial em Crimes Digitais Contra a Honra**. 2020. Disponível em: <<https://repositorio.ivc.br/handle/123456789/272?locale-attribute=en>>. Acesso em: 12 dez. 2025.

SOARES, Leonardo Humberto. A autoridade docente e a Sociedade da Informação: educação, crise e liquidez. 2016. Disponível em: <<https://www.semanticscholar.org/paper/Tecnologias-de-informa%C3%A7%C3%A3o-e-comunica%C3%A7%C3%A3o-para-a-para-Danielski-Prado/acf926bfad211811ad2a927aa1dc011337acca1>>. Acesso em: 29 dez. 2025.

SOARES, Victor Augusto Gonçalves. **Crimes informáticos**: os desafios enfrentados pelo Direito Penal na Era Digital. 2019. Disponível em: <<https://repositorio.ufrn.br/handle/123456789/51725>>. Acesso em: 11 dez. 2025.

SOUSA, Lucas Queiroga Nóbrega de. **Análise crítica do papel da vítima nos crimes cibernéticos e dos desafios do controle penal**. 2023. Disponível em: <<https://repositorio.ufpb.br/jspui/handle/123456789/29440?locale=en>>. Acesso em: 12 dez. 2025.

TAVARES, Alexandre Nicola Soares de Souza. A PROTEÇÃO DA DEMOCRACIA COMO UM BEM JURÍDICO E SUA IMPORTÂNCIA NO DIREITO PENAL. **Revista Jurídica do Nordeste Mineiro**, v. 12, n. 1, 2024. Disponível em: <<https://jrnrm.ojsbr.com/juridica/article/view/2968>>. Acesso em: 04 out. 2025.

TENÓRIO, José Rubens Arcanjo. Interpretação extensiva no âmbito do direito penal e o princípio da legalidade, sob o prisma da teoria garantista. 2022. Disponível em: <<https://www.repositorio.ufal.br/bitstream/123456789/11124/1/Interpreta%C3%A7%C3%A3o%20extensiva%20no%20%C3%A2mbito%20do%20direito%20penal%20e%20o%20princ%C3%ADpio%20da%20legalidade%2C%20sob%20o%20prisma%20da%20teoria%20garantista.pdf>>. Acesso em: 12 dez. 2025.

TRIVINO, Aline Melsone Marcondes. **Crimes cibernéticos**: como a nova tecnologia desafia o Direito Penal. 2024. Disponível em: <<https://repositorio.pucsp.br/jspui/handle/handle/41316>>. Acesso em: 24 out. 2025.

VALENTE, Manuel Monteiro Guedes. O reforço dos princípios constitucionais na obtenção de prova no mundo digital. **Revista de Direito de Polícia Judiciária**, v. 2, n. 3, p. 11-25, 2018. Disponível em: <https://www.researchgate.net/publication/348144804_O_Reforco_dos_Principios_Constitucionais_na_Obtencao_de_Prova_no_Mundo_Digital>. Acesso em: 16 nov. 2025.

VELOSO FILHO, José Carlos. **Direito Penal e Processual Penal em perspectiva**: contribuições crítico-reflexivas para o avanço do Sistema de Justiça Criminal. 2025. Disponível em: <<https://repositorio.uniceub.br/jspui/handle/prefix/17689>>. Acesso em: 12 dez. 2025.

VIANA, Eduardo. Observações sobre o princípio da legalidade. **Revista Científica do CPJM**, v. 1, n. 02, p. 96-125, 2021. Disponível em: <<https://rcpjm.cpj.m.uerj.br/revista/article/view/36>>. Acesso em: 29 dez. 2025.

VILAÇA, Márcio Luiz Corrêa; ARAÚJO, Elaine Vasquez Ferreira de. **Tecnologia, sociedade e educação na era digital**. Duque de Caxias: UNIGRANRIO, 2016. Disponível em: <<https://marciovilaca.com.br/digital/tag/tecnologia/>>. Acesso em: 12 out. 2025.

WERTHEIN, Jorge. A sociedade da informação e seus desafios. **Ciência da Informação**, Brasília, v. 29, n. 2, p. 71-77, maio/ago. 2000. Disponível em: <<https://www.scielo.br/j/ci/a/rmmLFLLbYsjPrkNrbkrK7VF/?format=pdf&lang=pt>>. Acesso em: 12 dez. 2025.

XAVIER, Pedro Paulo Cunha. **CRIMES CIBERNÉTICOS: DESAFIOS E PERSPECTIVAS NA ERA DIGITAL**. 2025. Disponível em: <<https://repositorio.pucgoias.edu.br/jspui/handle/123456789/9187>>. Acesso em: 29 set. 2025.