FACULDADE DE DIREITO DO SUL DE MINAS

DEYBER DA SILVA URBANO

OS DESAFIOS DO DIREITO PENAL PARA LIDAR COM OS CRIMES CIBERNÉTICOS À LUZ DO PRINCÍPIO CONSTITUCIONAL DA LEGALIDADE

MINAS GERAIS

2025

FACULDADE DE DIREITO DO SUL DE MINAS

DEYBER DA SILVA URBANO

OS DESAFIOS DO DIREITO PENAL PARA LIDAR COM OS CRIMES CIBERNÉTICOS À LUZ DO PRINCÍPIO CONSTITUCIONAL DA LEGALIDADE

Dissertação de Mestrado apresentada à Banca Examinadora da Faculdade de Direito do Sul de Minas, como exigência parcial para a obtenção do título de Mestre em Direito, sob orientação do Prof. Pos-Dr. Rafael Lazzarotto Simioni

MINAS GERAIS

2025

FICHA CATALOGRÁFICA

U733o URBANO, deyber silva

Os Desafios do Direito Penal pra lidar com Crimes Cibernéticos a luz do Principio Constitucional da Legalidade / deyber silva urbano. Pouso Alegre: FDSM, 2025.

105p.

Orientador: Rafael Lazzarotto Simioni.

Dissertação (Mestrado) - Faculdade de Direito do Sul de Minas, Programa de Pós-Graduação em Direito.

1. Crimes Cibernéticos. 2. Tipicidade Penal. 3. Legalidade.

I. Simioni, Rafael Lazzarotto . II. Faculdade de Direito do Sul de Minas. III. Título.

CDU 340

RESUMO

A pesquisa analisa a incidência dos crimes cibernéticos em geral, à luz do princípio constitucional da legalidade. O estudo parte da constatação de que o avanço tecnológico criou novas formas de interação e também novos riscos, desafiando o Direito Penal a se adaptar sem violar suas garantias fundamentais. O objetivo geral foi compreender de que modo o princípio da legalidade pode orientar a tipificação e a persecução penal de condutas digitais complexas. Utilizou-se metodologia qualitativa, de natureza exploratória e analítica, com revisão bibliográfica e exame de marcos legislativos nacionais e internacionais. Os resultados demonstram que a criação de tipos penais específicos é necessária para abranger condutas cibernéticas próprias, garantindo segurança jurídica e previsibilidade normativa. Observou-se, ainda, que a norma penal em branco pode ter aplicação limitada em questões técnicas, desde que não transfira ao poder regulamentar o núcleo da proibição penal. Conclui-se que o equilíbrio entre legalidade, inovação e proporcionalidade é essencial para a construção de um Direito Penal digital efetivo e constitucionalmente legítimo.

Palavras-chave: Tipicidade Penal. Crimes Cibernéticos. Legalidade. Norma Penal em Branco.

ABSTRACT

The research analyzes the incidence of cybercrimes in general in light of the constitutional principle of legality. The study starts from the observation that technological progress has created new forms of interaction and risk, challenging Criminal Law to adapt without violating its fundamental guarantees. The general objective was to understand how the principle of legality can guide the typification and prosecution of complex digital conducts. The methodology adopted was qualitative, exploratory, and analytical, based on bibliographic review and examination of national and international legal frameworks. The results demonstrate the need to create specific criminal types to address proper cybercrimes, ensuring legal certainty and normative predictability. It was also observed that the "blank criminal norm" may apply to technical aspects, provided that the core of the offense remains defined by law. The study concludes that balancing legality, innovation, and proportionality is essential for developing an effective and constitutionally legitimate digital Criminal Law.

Keywords: Criminal Typicity. Cybercrimes. Legality. Blank Criminal Norm.

SUMÁRIO

1 Introdução

A presente pesquisa insere-se na linha de investigação “Relações Sociais e Democracia”, tendo como enfoque a proteção dos direitos fundamentais no Estado Constitucional contemporâneo e os desafios impostos pelo avanço tecnológico. O princípio da legalidade, basilar ao Direito Penal, encontra-se tensionado diante das novas formas de criminalidade cibernética, que se caracterizam pela fluidez, pela transnacionalidade e pela constante mutação dos meios utilizados. Tal cenário exige reflexão sobre os limites e possibilidades da intervenção penal sem comprometer as garantias fundamentais do cidadão.

A pertinência desta linha de pesquisa justifica-se na medida em que os crimes virtuais, cada vez mais frequentes e sofisticados, representam ameaça concreta à segurança jurídica, à privacidade e à integridade do patrimônio das pessoas. Questões como o golpe do falso advogado, o golpe do Pix e diversas outras fraudes digitais vêm se popularizando e desafiando a atuação do Estado. Tais delitos, ao mesmo tempo em que demonstram a vulnerabilidade da sociedade em rede, evidenciam lacunas na tipicidade penal tradicional, suscitando discussões acerca da atualização normativa e da formulação de políticas públicas eficazes.

Nesse sentido, o primeiro eixo analítico aborda as novas espécies de crimes praticados por meio virtual, descrevendo os principais golpes em evidência e problematizando sua adequação ao princípio da legalidade. Em seguida, discute-se o modus operandi dos cibercriminosos, explorando técnicas como phishing, engenharia social, ataques distribuídos de negação de serviço (DDoS), ransomware e a comercialização de credenciais vazadas, destacando como esses mecanismos desafiam os contornos clássicos da tipicidade penal.

O terceiro ponto da investigação refere-se às formas de coibir e identificar o cibercriminoso, analisando os instrumentos legais disponíveis, como o Marco Civil da Internet, a Lei 9.296/1996 sobre interceptações, as normas do Código de Processo Penal sobre cadeia de custódia (arts. 158-A a 158-F), além da cooperação jurídica internacional consagrada pela Convenção de Budapeste e pelos acordos de assistência mútua (MLAT). A ênfase recai sobre os procedimentos técnicos e práticos necessários à persecução penal em ambiente digital.

Examinam-se as técnicas e meios alternativos para resolver casos em que o direito penal tradicional se mostra insuficiente, incluindo soluções de governança digital, regulação setorial, compliance tecnológico e colaboração entre Estado, setor privado e sociedade civil. Dessa forma, pretende-se contribuir para o debate acadêmico e prático acerca da atualização do Direito Penal e Processual Penal no enfrentamento dos crimes cibernéticos, sem violar o princípio da legalidade que constitui garantia fundamental em um Estado Democrático de Direito.

O presente estudo tem por base investigar a aplicabilidade da tipicidade penal às condutas criminosas praticadas no ambiente digital, com especial atenção à conformidade das respostas punitivas com o Princípio Constitucional da Legalidade que rege a Constituição Federal. A pesquisa se concentrará na análise da legalidade constitucional — reserva legal (somente a lei em sentido estrito pode criar crimes e penas), anterioridade da lei penal (a conduta somente pode ser punida se previamente definida como crime), proibição da analogia in malam partem (vedação de interpretação extensiva prejudicial ao réu) e segurança jurídica (garantia de previsibilidade das condutas puníveis, art. 5º, XXXIX, CF). Também serão considerados os reflexos desses princípios nos direitos fundamentais, como liberdade, privacidade, intimidade e devido processo legal, no contexto da sociedade em rede.

A partir disso, serão analisados os limites constitucionais para a criação de novos tipos penais em face da proteção de bens jurídicos na realidade digital, considerando o novo *modus operandi* dos cibercriminosos, que traz repercussões no espaço e no tempo, principalmente no tocante ao *locus delicti*. Torna-se, assim, necessária uma investigação sobre os reflexos dessa nova era tecnológica no campo penal.

Esse estudo baseia-se numa construção doutrinária e em interpretações variadas, buscando analisar como os tipos penais tradicionais, concebidos para a realidade física, enfrentam dificuldades para abarcar condutas cometidas em ambientes digitais, nos quais a separação entre o agente, o espaço virtual da conduta e os impactos reais torna nebulosa a aplicação dos critérios clássicos de subsunção penal.

O avanço tecnológico e a popularização de práticas digitais, como transações financeiras online, redes sociais, armazenamento em nuvem e serviços descentralizados, têm levantado questões complexas sobre a aplicação do direito penal. Nesse cenário, é crucial identificar e definir quais ações podem ser tipificadas como crimes em meio virtual, estabelecendo critérios para a definição legal de comportamentos que, no mundo real, já seriam considerados delitos[1].

Além disso, discute-se a questão da jurisdição e competência, diante da natureza global e descentralizada da internet, o que traz desafios para a investigação e o julgamento dos delitos. A adequação e eficácia da tipicidade penal para crimes cibernéticos também são analisadas, considerando quais normas incriminadoras seriam mais apropriadas e como garantir que tais medidas tenham efeito preventivo e orientador de condutas.

Aqui, aborda-se a cooperação internacional, explorando como as autoridades de

[1] ALECRIM, Emerson. Vírus de computador e outros malwares: o que são e como agem. Infowester. 2013.

diferentes países podem colaborar na investigação e persecução de crimes cibernéticos, dada a transnacionalidade dessas infrações. Ao tratar desses aspectos, a pesquisa busca fornecer um panorama crítico sobre os desafios e as possíveis soluções para a aplicação do Direito Penal em um dos contextos mais dinâmicos e complexos da contemporaneidade.

O problema central desta pesquisa consiste em saber em que medida o princípio constitucional da legalidade, aplicado ao Direito Penal, é capaz de conferir validade e segurança jurídica à tipificação de condutas delituosas praticadas no ambiente digital. Em um cenário marcado por inovação tecnológica disruptiva, globalização das relações e vulnerabilidade de direitos fundamentais, questiona-se a suficiência dos princípios tradicionais da tipicidade penal e da territorialidade para lidar com os desafios impostos pelos crimes cibernéticos, que se caracterizam pela fluidez, pela transnacionalidade e pela sofisticação de seus meios de execução.

A criminalidade virtual acrescenta uma nova camada de complexidade à aplicação do Direito Penal: como definir a tipicidade de condutas praticadas em ambiente digital que, embora muitas vezes imateriais, produzem efeitos concretos sobre pessoas, patrimônios e instituições no mundo real?

Especificamente, o estudo busca possíveis respostas às seguintes indagações:

- Como compatibilizar a criação ou adaptação de tipos penais às condutas digitais com os limites constitucionais da legalidade impostos ao poder punitivo estatal?
- Como assegurar, em meio digital, a observância do princípio da legalidade quando agentes, vítimas e efeitos das condutas se encontram pulverizados globalmente?
- O sistema penal brasileiro está constitucionalmente estruturado para enfrentar os desafios que emergem dos crimes transfronteiriços praticados em ambientes digitais descentralizados?
- Quais são os desafios enfrentados pelo Direito Penal para reconhecer e tipificar condutas como fraudes eletrônicas, golpes financeiros, ataques a sistemas e crimes contra a privacidade?
- É possível aplicar tipos penais tradicionais às ações realizadas em rede, como phishing, ransomware ou uso de credenciais vazadas?
- Como a instrumentalização da tecnologia da informação para fins criminosos impacta os critérios de tipicidade e a aplicabilidade territorial da norma penal?
- As legislações penais nacionais e internacionais estão preparadas para absorver

tais condutas cibernéticas em constante mutação?

- Quais propostas legislativas e doutrinárias têm surgido para a construção de novos tipos penais que abranjam de forma adequada os crimes virtuais contemporâneos?
- Como conciliar a criação de novos tipos penais com os princípios constitucionais da legalidade, anterioridade e taxatividade?

Assim o objetivo geral desta pesquisa foi: analisar a insuficiência dos princípios tradicionais da tipicidade penal frente aos novos desafios impostos pelos crimes cibernéticos, em consonância com o princípio constitucional da legalidade, identificando em que medida o Direito Penal brasileiro é capaz de oferecer respostas seguras e eficazes às condutas ilícitas praticadas no ambiente digital.

Como objetivos específicos, tais foram:

a) Examinar a aplicabilidade dos tipos penais clássicos às condutas praticadas em meios digitais, avaliando se há adequação ou necessidade de reformulação legislativa.
b) Analisar as propostas legislativas e doutrinárias recentes que tratam da construção de novos tipos penais voltados aos crimes cibernéticos, com destaque para os limites constitucionais da legalidade frente à inovação tecnológica.
c) Avaliar criticamente a necessidade de um novo marco legal penal direcionado à regulamentação de condutas ilícitas em ambientes digitais, considerando os aspectos de territorialidade, soberania jurídica e cooperação internacional.
d) Investigar como técnicas de investigação e instrumentos de cooperação internacional podem ser compatibilizados com as garantias constitucionais da legalidade e da segurança jurídica na persecução penal dos crimes cibernéticos.

A justificativa para a realização desta pesquisa decorre do impacto crescente dos crimes cibernéticos na sociedade contemporânea, os quais afetam desde relações interpessoais até a segurança econômica global. A disseminação de fraudes digitais, como o golpe do Pix e a atuação de falsos advogados em ambiente virtual, revela a urgência de compreender como o Direito Penal, limitado pelo princípio da legalidade, pode se adaptar a condutas cada vez mais sofisticadas e mutáveis. Nesse contexto, a pesquisa se mostra necessária para identificar em que medida os tipos penais clássicos são insuficientes diante da nova criminalidade informacional.

A complexidade dos delitos digitais está associada à sua anônima autoria, caráter descentralizado e abrangência transnacional, o que dificulta a aplicação das normas tradicionais de tipicidade e territorialidade penal. Assim, torna-se essencial analisar como os princípios constitucionais — especialmente legalidade, anterioridade e taxatividade — podem orientar a

construção ou atualização legislativa, sem comprometer as garantias fundamentais dos indivíduos. Como salienta Beal (2015)[2], a proteção de ativos de informação exige abordagens jurídicas e técnicas integradas, de modo que a regulação penal dialogue com práticas efetivas de segurança.

Além disso, a pesquisa se justifica pela necessidade de resguardar direitos fundamentais, como liberdade, privacidade, intimidade e devido processo legal, constantemente vulnerados no ambiente digital. A insuficiência normativa atual pode resultar em espaços de impunidade, nos quais criminosos virtuais se aproveitam da ausência de tipificação clara para explorar vulnerabilidades de sistemas e de pessoas. Como aponta Binicheski (2011)[3], a responsabilização dos atores digitais, inclusive provedores, é um aspecto central para estruturar um regime jurídico mais eficaz.

Outro elemento que sustenta esta pesquisa é a dimensão internacional dos crimes cibernéticos. Dada a natureza global da internet, a cooperação entre Estados torna-se indispensável, seja na produção legislativa convergente, seja na investigação criminal. A Convenção de Budapeste, por exemplo, constitui marco fundamental nesse processo, reforçando a necessidade de o Brasil alinhar-se a parâmetros tecnológicos neutros e de abrangência transfronteiriça. A análise desse contexto mostra a relevância de propor soluções que não se limitem à legislação nacional, mas que integrem mecanismos de cooperação mútua e de preservação da prova digital.

Esta pesquisa é justificada pela urgência de adaptar o sistema penal às novas realidades digitais, garantindo proteção efetiva aos usuários, fortalecimento da segurança jurídica e respeito ao princípio constitucional da legalidade. Ao abordar os limites e possibilidades da tipicidade penal diante dos crimes cibernéticos, a investigação busca contribuir tanto para o desenvolvimento doutrinário quanto para a formulação de políticas públicas e reformas legislativas que promovam maior eficácia na prevenção e repressão desse tipo de criminalidade.

A presente pesquisa adota uma abordagem qualitativa, de natureza exploratória e explicativa, com o objetivo de compreender, sob uma perspectiva crítica e dogmática, os limites e as possibilidades de aplicação do princípio constitucional da legalidade diante da tipificação penal dos crimes cibernéticos. O percurso metodológico fundamenta-se na revisão sistemática da literatura jurídica e na análise documental, privilegiando a interpretação teórica, normativa

[2] BEAL, Adriana. Segurança da informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações. São Paulo: Atlas, 2015.
[3] BINICHESKI, Paulo Roberto. Responsabilidade civil dos provedores de internet: direito comparado e perspectivas de regulação no direito brasileiro. São Paulo: Juruá, 2011.

e jurisprudencial do fenômeno estudado. A pesquisa bibliográfica concentra-se em obras e artigos científicos que discutem os conceitos de tipo penal, bem jurídico, tipicidade, elementos objetivos e subjetivos do delito, bem como os impactos das novas tecnologias sobre a dogmática penal contemporânea.

Para tanto, são mobilizados autores de referência no Direito Penal e no Direito Digital, nacionais e estrangeiros, a fim de construir um arcabouço teórico consistente que permita analisar criticamente a suficiência dos tipos penais tradicionais frente às condutas praticadas no ambiente digital. De forma complementar, desenvolve-se uma pesquisa documental, voltada ao exame de legislações nacionais e internacionais, projetos de lei, tratados e convenções relacionadas aos crimes cibernéticos, com especial atenção ao Marco Civil da Internet (Lei nº 12.965/2014), à Lei nº 9.296/1996, às disposições do Código de Processo Penal sobre cadeia de custódia da prova digital (arts. 158-A a 158-F) e à Convenção de Budapeste.

Também são considerados casos paradigmáticos envolvendo fraudes digitais, golpes eletrônicos e ataques cibernéticos, a partir da análise de decisões judiciais e manifestações ministeriais, como forma de identificar tendências interpretativas e dificuldades práticas na aplicação da tipicidade penal. A coleta dos dados bibliográficos ocorre em bases reconhecidas, como SciELO, Google Acadêmico e Biblioteca Virtual em Saúde (BVS), utilizando descritores relacionados ao Direito Penal Digital. O tratamento das informações é realizado por meio de análise crítica e sistematizada, permitindo identificar lacunas normativas, riscos de expansão indevida do poder punitivo e os limites constitucionais que devem orientar eventuais propostas de aperfeiçoamento legislativo e político-criminal.

2 Os desafios do direito penal frente à criminalidade cibernética e o princípio da legalidade

As grandes revoluções no mundo são testemunhos poderosos da capacidade humana de buscar e implementar mudanças fundamentais. Embora cada revolução tenha suas especificidades, todas compartilham um impulso comum: a busca por um futuro melhor e mais justo. Estudar essas revoluções nos permite entender melhor os processos históricos que moldaram o presente e as possibilidades para o futuro[4]

A criminalidade cibernética constitui um dos maiores desafios contemporâneos para o Direito Penal, uma vez que se desenvolve em um ambiente marcado pela constante mutação tecnológica e pela ausência de fronteiras físicas. A cada nova inovação digital surgem formas inéditas de prática delitiva, como fraudes eletrônicas, golpes financeiros online, ataques a sistemas informáticos e violações de dados pessoais. Esses fenômenos, ao mesmo tempo em que impactam diretamente bens jurídicos como patrimônio, honra e privacidade, tensionam a estrutura clássica do Direito Penal, especialmente no que diz respeito ao princípio da legalidade e à exigência de taxatividade na criação de tipos penais.

Nesse cenário, o legislador enfrenta a difícil tarefa de elaborar normas que sejam eficazes para punir condutas em rápida transformação, sem abrir margem para interpretações extensivas que possam comprometer garantias constitucionais. O dilema consiste em conciliar a necessidade de proteção da sociedade diante das novas modalidades de crime com a observância estrita do preceito constitucional de que não há crime nem pena sem lei anterior que o defina. Assim, a análise dos desafios impostos pela criminalidade cibernética demanda uma reflexão crítica sobre os limites e as possibilidades do Direito Penal em um contexto de inovação tecnológica permanente.

2.1 Novas espécies de crimes virtuais e sua tipificação penal

O golpe do falso advogado é uma das fraudes digitais que mais têm chamado a atenção das autoridades nos últimos anos. Nele, criminosos se passam por profissionais do direito,

[4] IRIBURE JÚNIOR, Hamilton da Cunha; MARTINS, José Renato; SILVA, Douglas de Morais (Coords.). Direitos fundamentais: multiculturalismo e tecnologia na sociedade globalizada. São Paulo: Saraiva, 2018. Pag. 16

utilizando informações previamente coletadas ou manipuladas para convencer vítimas de que estão em situações processuais urgentes, exigindo pagamentos imediatos para evitar supostas penalidades. Essa conduta explora a fragilidade emocional de pessoas que, em estado de aflição, acabam transferindo recursos sem verificar a veracidade da situação. O uso da tecnologia nesse tipo de estelionato revela como o cibercrime não depende apenas de ferramentas sofisticadas, mas também da manipulação psicológica, característica típica da engenharia social, o que reforça a necessidade de políticas públicas de conscientização digital e instrumentos normativos atualizados[5].

Outro crime de grande repercussão é o golpe do Pix, que se aproveita da rapidez e da irreversibilidade das transferências realizadas pelo sistema de pagamentos instantâneos. Os criminosos utilizam mensagens falsas enviadas por aplicativos, perfis clonados ou até mesmo invasão de contas bancárias digitais para induzir as vítimas a transferirem valores que, uma vez enviados, dificilmente são recuperados. Esse golpe expõe uma vulnerabilidade estrutural do sistema financeiro digital, pois combina a engenharia social com falhas de autenticação e de monitoramento das instituições. Além disso, o fenômeno levanta questões importantes sobre a necessidade de legislação que acompanhe a inovação tecnológica, garantindo equilíbrio entre celeridade nas transações e segurança dos usuários[6].

As fraudes bancárias eletrônicas, igualmente recorrentes, constituem modalidade criminosa que engloba invasões de contas, instalação de malwares, interceptação de dados de cartões e uso indevido de informações pessoais para realização de transações ilícitas. A sofisticação dessas práticas desafia os mecanismos tradicionais de investigação, pois muitas vezes os ataques são realizados por redes internacionais, dificultando a identificação dos autores. Nesse cenário, o Marco Civil da Internet surge como instrumento normativo fundamental, ao estabelecer princípios para a preservação e fornecimento de dados mediante ordem judicial, garantindo que a persecução penal se dê em conformidade com a legalidade e com o devido processo. A norma, além de fortalecer a proteção da privacidade, também fornece bases jurídicas indispensáveis para responsabilizar agentes que exploram falhas digitais[7].

Outro golpe que se disseminou no cotidiano é a clonagem de aplicativos de mensagens,

---

[5] BARBOSA, Luana Cristhine Oliveira; CEZAR, André Althmann; CARVALHO, Thomaz Jefferson. A evolução do direito penal frente às novas tecnologias e o crime de estupro virtual. Anais Eletrônico ISBN 978-65-5615-164-9 X Mostra Interna de Trabalhos de Iniciação Científica III Mostra Interna de Trabalhos de Iniciação em Desenvolvimento Tecnológico e Inovação. 2024. p. 15.

[6] HERNANDEZ, Erika Fernanda Tangerino; DE TOLEDO, Nathália Karina Abucci. Crimes cibernéticos: seus efeitos revolucionários diante de uma legislação em constante evolução. Revista Jurídica da UniFil, v. 17, n. 17, p. 72-84, 2021. p. 76.

[7] BRASIL. Marco Civil da Internet (Lei nº 12.965, de 23 de abril de 2014). Brasília: Presidência da República. p. 22.

especialmente o *WhatsApp,* em que criminosos conseguem assumir a identidade digital de usuários para enganar seus contatos. A partir dessa apropriação, são enviadas mensagens solicitando transferências financeiras ou compartilhamento de informações sigilosas, explorando a confiança já existente entre as partes. Essa prática demonstra que a fragilidade não está apenas na tecnologia, mas no vínculo interpessoal que é manipulado pelo criminoso. Além de causar danos patrimoniais imediatos, a clonagem gera impactos emocionais significativos, uma vez que a vítima se sente exposta e traída em sua rede de relações. Por isso, é urgente que a legislação tipifique de maneira clara essas condutas, a fim de evitar a impunidade e fortalecer a segurança digital no país[8].

O estelionato digital, em especial, evidencia o processo de adaptação de crimes tradicionais ao ambiente virtual. A prática, que no mundo físico se fundamentava em falsas promessas e enganos diretos, no ciberespaço ganha novas roupagens, utilizando plataformas de comércio eletrônico, redes sociais e aplicativos financeiros. Esse deslocamento demanda que o Direito Penal se posicione de forma clara, evitando interpretações extensivas que possam ferir o princípio da legalidade, mas também evitando omissões que favoreçam criminosos. A ausência de clareza na definição normativa fragiliza a persecução penal, gerando insegurança jurídica para vítimas, magistrados e operadores do direito. Assim, a consolidação do estelionato digital como tipo penal específico representa passo importante para garantir segurança jurídica e eficácia na repressão[9].

Os crimes contra a honra praticados nas redes sociais representam outra categoria relevante da criminalidade digital. Nesse contexto, injúrias, calúnias e difamações são potencializadas pelo alcance quase ilimitado da internet, tornando-se públicas em questão de segundos e permanecendo disponíveis por tempo indeterminado. Diferente do que ocorre no espaço físico, em que a ofensa se restringe a um número reduzido de pessoas, no ambiente virtual os danos se multiplicam em escala e intensidade. Essa nova dimensão do crime exige um posicionamento cuidadoso do Direito, pois envolve o desafio de conciliar a proteção da dignidade da pessoa humana com a preservação da liberdade de expressão, valor igualmente protegido pela Constituição[10].

Autores da área de segurança digital e relatos de *ex-hackers* reforçam como a

---

[8] MOTA, Carlos Henrique De Espindola. Cyberstalking: a necessidade de tipificação no direito penal brasileiro. *Portal de Trabalhos Acadêmicos,* v. 12, n. 1, 2020. p. 41.

[9] TAVARES, Juarez. Projeto de Código Penal: a reforma da parte geral. Revista da EMERJ, v. 15, n. 60, p. 161-189, 2012. p. 168.

[10] BARROSO, Luís Roberto. *Curso de direito constitucional contemporâneo: os conceitos fundamentais e a construção do novo modelo*. 7. ed. São Paulo: Saraiva Educação, 2018. ISBN 9788547230869. p. 421.

manipulação psicológica permanece sendo um dos principais vetores de ataque. Muitas das invasões e fraudes realizadas não dependeram de conhecimentos técnicos avançados, mas da habilidade de explorar a ingenuidade ou desatenção de usuários e funcionários de empresas. Essa constatação reforça que, em muitos casos, o elo mais frágil da segurança não é a tecnologia em si, mas o fator humano, o que evidencia a necessidade de políticas educativas e de conscientização digital[11].

Estudos recentes também chamam atenção para a insuficiência da legislação vigente no enfrentamento da criminalidade virtual. Santana destaca que a falta de precisão normativa gera divergências interpretativas, dificultando a aplicação efetiva do Direito Penal e criando um ambiente de insegurança jurídica. Segundo o autor, o aprimoramento da tipificação penal é medida urgente para garantir que novas modalidades de crimes cibernéticos sejam enfrentadas de maneira eficaz, preservando, ao mesmo tempo, o princípio da legalidade e os direitos fundamentais[12].

É necessário reconhecer que os crimes digitais, em suas diversas modalidades, representam não apenas ameaças patrimoniais, mas também desafios de ordem constitucional e dogmática. Ao tensionarem o princípio da legalidade, obrigam o legislador e os tribunais a refletirem sobre os limites da intervenção penal em um ambiente em constante transformação. Esse panorama evidencia que a luta contra a criminalidade virtual não pode se restringir a reformas legislativas pontuais, mas deve envolver também cooperação internacional, fortalecimento da segurança cibernética e integração entre os diversos atores sociais[13].

A criminalidade cibernética apresenta-se como fenômeno em constante mutação, com práticas que rapidamente se adaptam às evoluções tecnológicas. Essa dinamicidade dificulta a criação de tipos penais estáveis e claros, pois a lei, necessariamente mais lenta em seu processo de elaboração, não acompanha a velocidade das transformações digitais. O resultado é uma tensão entre o princípio da legalidade, que exige previsão clara e anterior do crime, e a necessidade prática de responder a condutas cada vez mais sofisticadas[14].

Outro desafio consiste na identificação de elementos objetivos e subjetivos das condutas praticadas em rede. Muitos crimes digitais ocorrem sem contato físico direto, o que gera

---

[11] CHAIKLIN, 2012, p. 53.
[12] SANTANA, Gabriel Côvolo. Crimes cibernéticos: necessidade do aprimoramento da tipificação penal dos crimes cibernéticos. Artigo Científico apresentado à disciplina Trabalho de Curso II, da Escola de Direito, Negócios e Comunicação, Curso de Direito, da Pontifícia Universidade Católica de Goiás (PUCGOIÁS). 2021., p. 7.
[13] HERNANDEZ; TOLEDO, 2021, p. 80.
[14] SILVA, Fernanda Bílio et al. A tipificação das condutas praticadas em ambiente virtual. NOVOS DIREITOS, v. 10, n. 1, p. 74-88, 2023. p. 76.

dúvidas sobre a consumação, a tentativa e a autoria. Esse aspecto é perceptível em delitos como o cyberstalking, em que a perseguição é realizada por meios digitais e pode se prolongar indefinidamente. A correta qualificação penal dessas condutas exige reflexão sobre conceitos clássicos de crime permanente e continuado, aplicados em um contexto virtual[15].

A diversidade de práticas criminosas digitais também revela lacunas legislativas que afetam a segurança jurídica. Condutas como a criação de perfis falsos para difamação, a divulgação de imagens íntimas sem consentimento e o estupro virtual ainda encontram resistência em sua subsunção aos tipos penais existentes. A dificuldade decorre da ausência de contato físico, que em alguns delitos era elemento essencial, exigindo, portanto, atualização interpretativa ou legislativa[16].

O crime de estupro virtual é exemplo claro dessa problemática, pois consiste em constranger a vítima, mediante ameaça ou ardil, a praticar atos de natureza sexual em frente a uma câmera, sem que haja contato físico. Apesar do impacto psicológico e moral equivalente ao estupro tradicional, a ausência de previsão expressa gera insegurança quanto à sua tipificação. A jurisprudência tem buscado soluções, mas a falta de clareza legal compromete a previsibilidade e, consequentemente, o próprio princípio da legalidade[17].

Outro ponto de tensão refere-se à cadeia de custódia da prova digital. O Código de Processo Penal, após a Lei nº 13.964/2019, passou a dispor sobre os artigos 158-A a 158-F, estabelecendo requisitos para a preservação da integridade da prova. Contudo, no âmbito cibernético, os vestígios podem ser facilmente manipulados, deletados ou replicados, o que aumenta a dificuldade de sua validação em juízo. A tipicidade, nesse caso, encontra-se ameaçada pela fragilidade na coleta e conservação da prova digital[18].

No plano internacional, a Convenção de Budapeste e seu Protocolo Adicional (CETS 189) demonstram a necessidade de uma legislação com vocabulário tecnológico neutro, capaz de abranger diferentes condutas sem depender da forma exata como o crime é cometido. Essa perspectiva busca reduzir a defasagem entre inovação criminosa e legislação, oferecendo

---

[15] OLIVEIRA, Mozart Gustavo Faria de. Repensando os tipos penais do crime permanente, crime instantâneo de efeito permanente e do crime continuado no âmbito da rede mundial de computadores e redes sociais. Qual a melhor forma de qualificação do stalking agora previsto no Art. 147 A do Código Penal Brasileiro? 2023. 71 f. Trabalho de Conclusão de Curso (Bacharelado em Direito) - Faculdade Nacional de Direito, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2023. p. 44.

[16] SILVA, Maria Gabriella Lira Barboza. Crime cibernético: o crime de estupro virtual e a ausência do contato físico para tipificação. Portal de Trabalhos Acadêmicos, v. 13, n. 2, 2021. p. 82.

[17] SIQUEIRA, Kelly Cristyne Rodrigues. A tipificação do crime de estupro virtual no código penal brasileiro. Novos Direitos v.10, n.1, jan.- jun. 2023, p.74 - 88 ISSN: 2447 – 1631. 2024. p. 77.

[18] BRASIL, Código de Processo Penal, 2019.

padrões mínimos de criminalização aceitos internacionalmente[19].

A interceptação de comunicações telemáticas é outra ferramenta relevante para enfrentar crimes digitais, mas sua utilização também encontra barreiras no princípio da legalidade. A Lei nº 9.296/1996 prevê hipóteses estritas para esse procedimento, exigindo ordem judicial fundamentada. Entretanto, diante da sofisticação dos ataques, como o uso de criptografia e redes privadas, surge o dilema entre ampliar os poderes investigativos e preservar as garantias fundamentais dos cidadãos[20].

A falta de tipificação clara também é ressaltada em estudos que apontam para a dificuldade de enquadrar condutas digitais em categorias penais tradicionais. Bruno de Lucca Rodrigues Costa observa que a ausência de legislação específica faz com que práticas graves, como fraudes eletrônicas complexas, sejam tratadas sob tipos genéricos, como estelionato. Essa lacuna fragiliza a resposta penal e reforça a percepção de impunidade, estimulando a continuidade dos delitos[21].

A imprevisibilidade de novos delitos digitais gera insegurança tanto para os cidadãos, que não sabem claramente quais condutas são puníveis, quanto para os operadores do direito, que enfrentam dificuldades de enquadramento. Esse cenário exige um equilíbrio delicado entre atualização normativa e preservação de garantias constitucionais, para que o avanço da legislação não se transforme em violação do princípio da legalidade[22].

O uso de *ransomware* tornou-se uma das práticas mais preocupantes do cibercrime contemporâneo. Nesse tipo de ataque, os criminosos sequestram dados mediante criptografia e exigem o pagamento de resgate, muitas vezes em criptomoedas, para liberar o acesso. No Brasil, a conduta é geralmente enquadrada de forma indireta em crimes como extorsão ou dano informático, o que gera insegurança jurídica por não corresponder integralmente à gravidade da prática. Essa lacuna reforça a necessidade de criação de tipos penais específicos, capazes de enfrentar adequadamente a sofisticação tecnológica[23].

Outra conduta cada vez mais comum é a comercialização de credenciais vazadas em fóruns da dark web, onde senhas bancárias, logins de redes sociais e dados pessoais são vendidos em larga escala. Embora tais práticas tenham evidente potencial lesivo, ainda não

---

[19] CONSELHO DA EUROPA. Protocolo Adicional à Convenção de Budapeste (CETS 189) – Relatório Explicativo. Estrasburgo: Council of Europe, 2003.
[20] BRASIL, Lei nº 9.296, 1996.
[21] COSTA, Bruno de Lucca Rodrigues. Crimes virtuais: uma análise da falta de tipificação legal dos crimes cibernéticos. Monografia Jurídica apresentada à disciplina Trabalho de Curso II, da Escola de Direito e Relações Internacionais, Curso de Direito, da Pontifícia Universidade Católica de Goiás (PUCGOIÁS). 2021. p. 12.
[22] SILVA et al., 2023, p. 84.
[23] VICENTE, 2022, p. 14.

existe tipificação clara no ordenamento jurídico brasileiro, o que leva a um enquadramento forçado em figuras como furto ou estelionato. Essa imprecisão gera fragilidade no processo penal e contribui para a sensação de impunidade[24].

Os ataques distribuídos de negação de serviço (DDoS) também se tornaram uma ameaça significativa, uma vez que paralisam servidores e serviços essenciais ao sobrecarregá-los com requisições massivas. Apesar de seu impacto na economia digital e na segurança de informações sensíveis, esses ataques ainda não possuem previsão penal expressa no Brasil. A ausência de um tipo penal específico obriga operadores do direito a recorrerem a analogias perigosas, o que viola o princípio da legalidade e compromete a segurança jurídica[25].

Outro exemplo é o avanço da engenharia social aplicada em aplicativos de mensagens, que explora a vulnerabilidade humana mais do que falhas técnicas. Golpes que envolvem clonagem de perfis ou mensagens fraudulentas tornaram-se comuns, exigindo das vítimas atenção redobrada e das autoridades, novas formas de tipificação. Essa manipulação psicológica evidencia que a fragilidade dos sistemas não está apenas na tecnologia, mas no próprio usuário, que se torna alvo direto da criminalidade digital[26].

O fenômeno dos crimes digitais também se amplia com a prática do *cyberstalking*, em que a perseguição reiterada ocorre por meios virtuais. Essa conduta traz impactos psicológicos profundos e contínuos às vítimas, mas enfrenta dificuldades de enquadramento em razão da ausência de previsão expressa por muitos anos. A tipificação recente ainda é insuficiente, sobretudo diante da dificuldade de caracterizar permanência e continuidade em ambiente virtual, o que exige atualização doutrinária e legislativa constante[27].

A dificuldade em distinguir claramente o que é crime e o que não é compromete a função preventiva da lei penal e fragiliza a segurança jurídica. Esse cenário exige uma resposta legislativa célere, que acompanhe a evolução tecnológica sem perder de vista os limites constitucionais impostos pelo princípio da legalidade[28].

2.2 Modus operandi e técnicas de atuação dos cibercriminosos

O *phishing* é uma das tipologias mais recorrentes no cenário da criminalidade

[24] COSTA, 2021, p. 11.
[25] CONSELHO DA EUROPA, 2001, p. 29.
[26] MITNICK; SIMON, 2003, p. 91.
[27] MOTA, 2020, p. 50.
[28] SANTANA, 2021, p. 9.

cibernética, caracterizando-se pelo envio de mensagens fraudulentas que simulam comunicações oficiais de instituições financeiras ou serviços digitais. A intenção é induzir a vítima a fornecer informações confidenciais, como senhas ou números de cartão. O ataque baseia-se no engano e na confiança, explorando a ingenuidade ou a falta de atenção do usuário, e tem se mostrado altamente eficaz. A amplitude desse crime revela a necessidade de constante atualização legislativa, pois a conduta muitas vezes se enquadra em tipos genéricos, como estelionato, sem contemplar suas especificidades tecnológicas[29].

A engenharia social é considerada o coração de muitos crimes virtuais, pois envolve manipular pessoas para que revelem informações sigilosas ou realizem ações prejudiciais. Kevin Mitnick, ex-hacker e especialista em segurança, relata que grande parte de suas invasões bem-sucedidas foi possibilitada não por falhas técnicas, mas pela exploração de vulnerabilidades humanas, como a confiança ou a falta de treinamento em segurança digital. Essa modalidade criminosa evidencia como a fronteira entre tecnologia e comportamento humano é determinante para compreender o alcance do cibercrime[30].

O ransomware desponta como uma das ameaças mais graves da atualidade, consistindo em um software malicioso que criptografa os arquivos da vítima e exige pagamento de resgate, geralmente em criptomoedas, para a liberação do acesso. Esse tipo de ataque, além de gerar grandes prejuízos financeiros, compromete serviços essenciais de empresas e órgãos públicos, colocando em risco a continuidade de atividades estratégicas. A ausência de legislação específica para lidar com a tipificação desse delito expõe lacunas no ordenamento jurídico brasileiro[31].

Outro ataque de destaque são os *Distributed Denial of Service* (DDoS), que consistem em sobrecarregar servidores com um volume massivo de requisições simultâneas, tornando-os indisponíveis para usuários legítimos. Esses ataques podem paralisar plataformas de e-commerce, bancos e até mesmo serviços públicos digitais, afetando diretamente a economia e a confiança social na infraestrutura tecnológica. A Convenção de Budapeste, ao tratar da criminalização de ataques contra sistemas, já prevê parâmetros internacionais para combater tais condutas[32].

---

[29] SILVA, 2021, p. 44.
[30] MITNICK, Kevin D.; SIMON, William L. A arte do engano: controlando o elemento humano da segurança. John Wiley & Sons, 2003, p. 88.
[31] VICENTE, Gabriel de Andrade. A tipificação do crime de ransomware no direito penal brasileiro. 2022. 31 f. Monografia (Graduação em Direito) - Escola de Direito, Turismo e Museologia, Universidade Federal de Ouro Preto, Ouro Preto, 2022. p. 12.
[32] FONSECA, Kelly Gonçalves et al. Estupro virtual e sua possível tipificação no código penal. Libertas Direito, v. 1, n. 2, 2020. p. 27.

O vazamento de credenciais tornou-se prática recorrente em fóruns da *dark web*, onde dados de acesso a contas de e-mail, redes sociais e bancos são comercializados. O acesso indevido a essas informações expõe vítimas a golpes financeiros, chantagens e invasões de privacidade. Embora a legislação brasileira contemple delitos como invasão de dispositivo informático, a comercialização de dados pessoais ainda carece de tipificação penal mais clara, demandando reformas que dialoguem com a Lei Geral de Proteção de Dados[33].

Os ataques digitais também se caracterizam pela multiplicidade de técnicas combinadas, o que dificulta a sua categorização em tipos penais rígidos. Fraga destaca que a prática criminosa moderna envolve não apenas a exploração de falhas técnicas, mas também a combinação de ferramentas automatizadas, malwares e redes de anonimato, que tornam a investigação mais complexa. Essa pluralidade evidencia como a inovação criminosa ultrapassa os limites da legislação tradicional, exigindo abordagens integradas de prevenção e repressão[34].

Casos de estupro virtual exemplificam como a ausência de contato físico não impede a consumação de condutas gravíssimas, que causam traumas e violam a dignidade da vítima. A pressão exercida por meio digital para que a vítima pratique atos sexuais em frente às câmeras ou envie imagens íntimas configura uma nova modalidade criminosa que ainda encontra dificuldades de tipificação. A ausência de previsão expressa coloca em risco a segurança jurídica e amplia as margens de impunidade[35].

Estudos recentes sobre o estupro virtual também revelam que sua prática pode envolver múltiplas estratégias digitais, desde engenharia social até o uso de dados obtidos por *phishing* para chantagear as vítimas. Nesse sentido, observa-se que a tipificação insuficiente e a falta de consenso doutrinário geram insegurança, exigindo maior atenção do legislador. Pesquisas apontam que a criminalização clara dessas condutas é fundamental para assegurar a proteção integral da dignidade sexual no ambiente digital[36].

Observa-se que as tipologias clássicas de ataques virtuais – *phishing*, engenharia social, *ransomware*, DDoS e vazamento de credenciais – demonstram a complexidade do fenômeno e a dificuldade de enquadramento no sistema penal brasileiro. Esses ataques tensionam o princípio da legalidade e revelam lacunas que comprometem a segurança jurídica, reforçando a importância de normas internacionais como a Convenção de Budapeste e da produção

[33] BRITO, Auriney. Direito penal informático. Saraiva Educação SA, 2017. p. 59.
[34] FRAGA, Bruno; VANGLLER, Thompson. Técnicas de invasão. Compilado a partir de videoaulas e pesquisas por Thompson Vangller; idealização do projeto por Bruno Fraga. Londres, 2017. 548 p. p. 212.
[35] MARODIN, Tayla Schuster. O crime de estupro virtual:(des) necessidade de tipificação pelo ordenamento jurídico brasileiro. 2021. Dissertação de Mestrado. Pontifícia Universidade Católica do Rio Grande do Sul. p. 67.
[36] FONSECA et al., 2020, p. 81.

acadêmica voltada para atualizar o Direito Penal frente à realidade digital.

A utilização de técnicas de anonimização e redes privadas virtuais (VPNs) representa um dos maiores entraves à persecução penal em crimes cibernéticos. Ao ocultar o endereço IP e mascarar a localização real do usuário, essas ferramentas dificultam a identificação da autoria e desafiam os mecanismos tradicionais de investigação criminal. Essa realidade tensiona diretamente os conceitos de territorialidade e jurisdição, exigindo novas formas de cooperação internacional e adaptações legislativas para garantir a efetividade do Direito Penal[37].

A experiência de hackers renomados demonstra como o anonimato é explorado para perpetuar crimes em escala global. A vulnerabilidade estrutural dos mecanismos de rastreamento e confirma a necessidade de o ordenamento jurídico considerar as particularidades tecnológicas do modus operandi digital[38].

Outro desafio relevante decorre do uso de criptomoedas como meio de pagamento em atividades ilícitas. O caráter descentralizado e pseudônimo desses ativos digitais dificulta o rastreamento das transações, permitindo que criminosos recebam valores oriundos de *ransomware*, extorsões e comércio ilegal de dados sem deixar rastros claros para autoridades. A ausência de uma regulação uniforme internacional sobre criptomoedas reforça a insegurança jurídica e amplia as dificuldades para a responsabilização penal[39].

A *dark web*, espaço da internet acessível apenas por navegadores específicos como o Tor, amplia ainda mais as dificuldades de persecução penal. Nesse ambiente, criminosos comercializam drogas, armas, dados pessoais e serviços de ciberataques, em um mercado global praticamente inacessível aos mecanismos tradicionais de investigação. A natureza descentralizada da rede e o uso de criptografia de ponta tornam o processo de coleta de provas ainda mais desafiador, ampliando as lacunas de tipificação penal[40].

Além disso, a produção e preservação de provas digitais encontram barreiras específicas quando o crime envolve técnicas avançadas de anonimização. O Código de Processo Penal brasileiro, ao estabelecer nos artigos 158-A a 158-F a necessidade de cadeia de custódia, reconhece a importância de garantir a integridade da prova. No entanto, no âmbito digital, a volatilidade dos dados e a facilidade de manipulação fragilizam a comprovação dos delitos em juízo, dificultando a responsabilização penal efetiva[41].

A qualificação jurídica de condutas também se mostra problemática diante do modus

---

[37] TAVARES, 2012, p. 170.
[38] CHAIKLIN, Harris. Ghost in the Wires. My Adventures as the World's Most Wanted Hacker. 2012.
[39] SANTANA, 2021, p. 8.
[40] SILVA et al., 2023, p. 80.
[41] BRASIL, Código de Processo Penal, 2019.

operandi digital. Crimes como o *stalking*, previstos no artigo 147-A do Código Penal, quando praticados em ambiente virtual, desafiam os conceitos clássicos de crime permanente e continuado. A necessidade de repensar a classificação desses delitos, considerando sua prática reiterada e a potencial perpetuidade em redes sociais, é um desafio que exige releituras doutrinárias para não comprometer a coerência da tipicidade penal[42].

No cenário internacional, o Protocolo Adicional à Convenção de Budapeste (CETS 189) apresenta soluções importantes ao propor padrões mínimos de criminalização de condutas digitais, sem depender da tecnologia específica utilizada. Essa abordagem permite lidar com a constante mutabilidade do modus operandi dos cibercriminosos, reforçando a necessidade de harmonização normativa entre os Estados para garantir eficácia às investigações[43].

A dificuldade de tipificação de crimes que utilizam anonimização, criptografia e redes privadas também se manifesta em condutas mais recentes, como o estupro virtual. A ausência de contato físico leva a debates sobre a configuração do tipo penal, evidenciando que o modus operandi digital desafia conceitos tradicionais e exige novas abordagens interpretativas. Essa lacuna coloca em risco a proteção da dignidade sexual e a segurança jurídica, demandando atualizações normativas urgentes[44].

Enquanto os primeiros utilizam recursos como VPNs, criptomoedas e *dark web* para escapar da persecução, o sistema de justiça permanece limitado por barreiras processuais e tecnológicas. A solução exige um equilíbrio entre inovação legislativa, respeito ao princípio da legalidade e fortalecimento da cooperação internacional, a fim de que a persecução penal não seja esvaziada diante da criminalidade cibernética[45].

2.3 Meios de investigação e superação das limitações do direito penal tradicional

A primeira ferramenta jurídica essencial no enfrentamento da criminalidade digital é o Marco Civil da Internet, que estabelece princípios fundamentais para o uso da rede no Brasil, incluindo a preservação e fornecimento de dados mediante ordem judicial. Esse instrumento é vital para a persecução penal, pois garante tanto a proteção da privacidade quanto a possibilidade de responsabilização de usuários que praticam delitos online. A preservação de

[42] OLIVEIRA, 2023, p. 55.
[43] CONSELHO DA EUROPA, 2003, p. 22.
[44] SIQUEIRA, 2024, p. 79.
[45] BARROSO, 2018, p. 433.

registros de conexão e de acesso a aplicações possibilita a reconstrução do caminho percorrido pelo cibercriminoso, servindo como ponto de partida para investigações técnicas[46].

Outro mecanismo relevante é a interceptação de comunicações, prevista na Lei nº 9.296/1996, que regula a captação de dados telefônicos e telemáticos mediante autorização judicial. Essa medida, embora excepcional, é indispensável diante da sofisticação das práticas criminosas, especialmente aquelas que utilizam criptografia para ocultar mensagens. O grande desafio está em equilibrar a eficácia investigativa com a preservação dos direitos fundamentais, garantindo que a medida seja aplicada em conformidade com os limites constitucionais[47].

A cadeia de custódia da prova digital, prevista nos artigos 158-A a 158-F do Código de Processo Penal, é outro elemento indispensável para assegurar a validade das investigações. Em crimes cibernéticos, onde dados podem ser facilmente alterados ou excluídos, o cumprimento rigoroso das etapas de coleta, guarda, transferência e análise é imprescindível para garantir a integridade da prova. Sem esse cuidado, qualquer evidência obtida pode ser desconsiderada em juízo, fragilizando a persecução penal[48].

No campo da cooperação internacional, a Convenção de Budapeste e seus mecanismos multilaterais de assistência jurídica (MLATs) oferecem parâmetros mínimos para harmonizar a criminalização e os procedimentos investigativos entre diferentes países. Essa cooperação é vital, pois a maior parte dos crimes digitais ultrapassa fronteiras nacionais, tornando ineficaz qualquer tentativa de persecução estritamente doméstica. A aplicação desses instrumentos fortalece a capacidade dos Estados em rastrear, identificar e responsabilizar agentes que atuam em ambientes descentralizados[49].

O uso de ferramentas tecnológicas pelas autoridades é igualmente fundamental. Investigações de *cyberstalking,* por exemplo, exigem monitoramento digital especializado e a análise de padrões de comportamento online. Ainda que o tipo penal já exista, sua efetividade depende da capacidade técnica dos órgãos de persecução em coletar, cruzar e validar dados que confirmem a habitualidade da perseguição no ambiente virtual. A dificuldade em rastrear perfis falsos ou mascarados mostra a relevância de protocolos técnicos avançados[50].

Casos como o estupro virtual evidenciam a importância da interação entre doutrina e tecnologia. A ausência de contato físico direto não impede a prática de constrangimentos graves

[46] BRITO, 2017, p. 63.
[47] BRASIL, Lei nº 9.296, 1996.
[48] TAVARES, 2012, p. 178.
[49] HERNANDEZ; TOLEDO, 2021, p. 80.
[50] MOTA, 2020, p. 47.

no ambiente digital, mas gera obstáculos na tipificação e na identificação do agressor. A coleta de evidências em plataformas privadas, bem como o uso de perícia em imagens e registros eletrônicos, torna-se essencial para que haja responsabilização penal efetiva, evitando a impunidade[51].

A literatura também aponta para a necessidade de novas abordagens diante das lacunas legislativas. Kelly Gonçalves Fonseca observa que o atraso na tipificação de condutas digitais, como o estupro virtual, gera insegurança jurídica e dificulta a coleta de provas. A ausência de previsão clara obriga magistrados e promotores a recorrerem a analogias arriscadas, o que pode ferir o princípio da legalidade. O fortalecimento de normas específicas é, portanto, uma medida imprescindível para coibir práticas emergentes[52].

Outro aspecto central é a atuação dos provedores de internet e plataformas digitais, cuja colaboração é indispensável para localizar e identificar criminosos. Pesquisas recentes indicam que a falta de integração entre esses atores e as autoridades de investigação retarda a obtenção de provas, comprometendo a efetividade das apurações. A criação de protocolos mais ágeis e seguros para compartilhamento de dados é apontada como medida necessária para enfrentar a criminalidade transnacional[53].

O equilíbrio entre repressão e garantias fundamentais deve nortear o uso de técnicas de investigação e cooperação. O princípio da legalidade continua a ser o fio condutor do sistema penal, assegurando que o combate ao crime digital não resulte em violações de direitos básicos dos cidadãos. Essa reflexão demonstra que coibir e identificar o cibercriminoso exige um sistema normativo claro, técnicos especializados e uma base ética sólida[54].

O enfrentamento da criminalidade cibernética não pode se restringir ao Direito Penal, já que a repressão tradicional se mostra insuficiente diante da mutabilidade das condutas digitais. Políticas públicas de cibersegurança constituem uma medida essencial, pois atuam de forma preventiva, fortalecendo a infraestrutura tecnológica e conscientizando a população sobre os riscos digitais. Essas políticas devem contemplar programas educativos, campanhas de sensibilização e investimentos em centros especializados de resposta a incidentes[55].

O compliance corporativo também se tornou peça-chave na contenção de ilícitos cibernéticos. Empresas que adotam práticas de governança digital, auditorias internas e

[51] MARODIN, 2021, p. 72.
[52] FONSECA et al., 2020, p. 83.
[53] BARBOSA; CEZAR; CARVALHO, 2024, p. 22.
[54] SILVA, 2021, p. 86.
[55] BRITO, 2017, p. 69.

protocolos de segurança conseguem minimizar riscos e identificar irregularidades com maior rapidez. Além de reduzir a exposição a ataques, tais mecanismos auxiliam na criação de uma cultura organizacional voltada à ética e à proteção de dados, complementando a atuação do Estado no combate ao cibercrime[56].

A regulação tecnológica é outro instrumento relevante, pois cria parâmetros mínimos de segurança que devem ser seguidos por empresas e usuários. Normas que impõem requisitos de proteção de dados, criptografia obrigatória em determinados serviços e notificações de incidentes fortalecem a confiança no ambiente digital. Contudo, a regulação deve ser equilibrada, evitando exageros que inviabilizem a inovação e respeitando os princípios constitucionais da legalidade e da proporcionalidade[57].

A cooperação público-privada representa um mecanismo indispensável para enfrentar crimes cibernéticos, uma vez que os provedores de serviços digitais detêm informações cruciais para investigações. A construção de canais de comunicação ágeis entre autoridades policiais, Ministério Público e empresas de tecnologia é condição essencial para a eficácia das apurações. Essa colaboração deve ser acompanhada de garantias jurídicas claras para assegurar o respeito à privacidade e aos direitos fundamentais dos usuários[58].

Os instrumentos de governança digital, por sua vez, ampliam a capacidade de prevenção ao estabelecer padrões de conduta, protocolos de resposta e mecanismos de auditoria sobre o uso da tecnologia. Tais instrumentos fortalecem a responsabilidade compartilhada entre Estado, setor privado e sociedade civil, garantindo maior resiliência frente a ataques coordenados. Além disso, servem como forma de reduzir a dependência exclusiva do sistema penal, criando uma abordagem integrada[59].

Casos de *cyberstalking* mostram a importância de soluções complementares, pois a perseguição digital pode ser contínua e difícil de coibir apenas com instrumentos penais. Políticas de prevenção, como bloqueio automático de perfis abusivos, monitoramento por inteligência artificial e programas de proteção a vítimas, reforçam a eficácia da resposta jurídica. Assim, a conjugação entre técnicas de segurança digital e medidas legislativas cria um ambiente mais seguro para os usuários[60].

---

[56] VICENTE, 2022, p. 15.
[57] BARROSO, 2018, p. 440.
[58] SANTANA, 2021, p. 10.
[59] SOUZA, Luiza Ananda Queiroz; CERVINSKI, Yasmin. É POSSÍVEL A PREVENÇÃO E COMBATE AOS TEMIDOS CRIMES VIRTUAIS?. Anuário Pesquisa e Extensão Unoesc São Miguel do Oeste, v. 6, p. e27776-e27776, 2021. p. 5.
[60] MOTA, 2020, p. 52.

A experiência internacional, sobretudo a partir da Convenção de Budapeste, demonstra que o combate ao cibercrime exige padrões globais e medidas além da esfera penal. O tratado enfatiza a necessidade de harmonização legislativa e da adoção de boas práticas técnicas, como logs de preservação de dados e cooperação imediata entre autoridades competentes. Esses mecanismos reduzem a fragmentação das respostas nacionais e aumentam a efetividade das investigações transnacionais[61].

Muitos crimes poderiam ser evitados se usuários e funcionários estivessem treinados para reconhecer tentativas de engenharia social e *phishing*. Essa perspectiva reforça que, além da regulação e da repressão penal, a educação digital é um dos caminhos mais eficazes para mitigar riscos e proteger bens jurídicos[62].

A efetividade da persecução penal em crimes cibernéticos também depende do fortalecimento da perícia digital. A atuação de peritos especializados na análise de dispositivos eletrônicos, redes e sistemas é fundamental para identificar vestígios técnicos que possam servir como prova em juízo. Sem esse trabalho, a apuração de crimes complexos como *ransomware* ou fraudes bancárias digitais fica comprometida, gerando risco de impunidade[63].

A doutrina também destaca que a investigação digital não deve se restringir à fase repressiva, mas deve contemplar estratégias preventivas articuladas com a sociedade civil e o setor privado. Kelly Gonçalves Fonseca observa que a ausência de tipificação adequada em casos de estupro virtual revelou não apenas a fragilidade da legislação, mas também a falta de protocolos de prevenção em plataformas digitais. Essa ausência amplia a vulnerabilidade das vítimas e dificulta a produção de provas[64].

O papel da cooperação internacional é reforçado pela crescente descentralização das condutas criminosas. A Convenção de Budapeste trouxe avanços ao propor padrões uniformes de criminalização e mecanismos de assistência mútua entre países. Entretanto, sua efetividade depende do engajamento real dos Estados signatários e da atualização constante dos protocolos, já que as práticas criminosas digitais evoluem em ritmo acelerado[65].

A responsabilidade compartilhada entre Estado, empresas de tecnologia e usuários também é elemento central na construção de um sistema de segurança digital robusto. Auriney Brito enfatiza que o Direito Penal deve atuar em conjunto com políticas de governança digital

[61] CONSELHO DA EUROPA, 2001, p. 39.
[62] MITNICK; SIMON, 2003, p. 92.
[63] MARODIN, 2021, p. 65.
[64] FONSECA et al., 2020, p. 82.
[65] CONSELHO DA EUROPA, 2001, p. 42.

e medidas técnicas, de modo a evitar que a repressão penal se torne inócua diante da sofisticação do modus operandi criminoso. Esse modelo integrado é o que garante maior eficácia no enfrentamento do cibercrime[66].

3 Marco legal dos crimes cibernéticos

O avanço exponencial das tecnologias digitais impôs ao Direito Penal um desafio inédito: acompanhar, com precisão normativa, a velocidade das transformações cibernéticas. A globalização da informação e a interconexão de sistemas criaram novas formas de criminalidade, exigindo um marco jurídico capaz de proteger bens jurídicos no ambiente virtual com a mesma eficácia garantida no espaço físico. No Brasil, o marco legal dos crimes cibernéticos consolida-se por meio de um conjunto de leis, tratados e princípios que buscam compatibilizar a repressão penal com o respeito aos direitos fundamentais, especialmente o princípio da legalidade. Essa estrutura normativa é fruto de um processo de amadurecimento legislativo que alia a tutela penal à cooperação internacional e à segurança digital.

Nesse contexto, o presente capítulo tem por objetivo analisar os principais instrumentos legais aplicáveis à criminalidade cibernética, tanto no âmbito nacional quanto internacional. Serão examinadas as leis brasileiras que introduziram a responsabilização penal de condutas virtuais, como a Lei nº 12.737/2012 e o Marco Civil da Internet, além da relevância da Lei Geral de Proteção de Dados para a preservação da privacidade e da integridade informacional. Também serão abordados os tratados internacionais, com destaque para a Convenção de Budapeste, e as propostas de reforma legislativa que buscam aprimorar a tipificação penal diante de novas modalidades de ataque digital. O estudo busca, portanto, compreender a coerência e os desafios desse arcabouço normativo frente à complexidade dos delitos virtuais e à necessidade de adaptação do Direito Penal à era digital.

3.1 Legislação penal brasileira aplicável aos crimes digitais

A promulgação das Leis nº 12.737/2012 e nº 12.735/2012 marcou um divisor de águas na responsabilização penal das condutas ilícitas praticadas no ambiente digital. A primeira, popularmente conhecida como Lei Carolina Dieckmann, tipificou delitos relacionados à invasão de dispositivos eletrônicos, ao passo que a segunda determinou a criação de delegacias especializadas em crimes cibernéticos. Ambas representaram o início de uma adaptação

[66] BRITO, 2017, p. 71.

legislativa necessária diante da crescente sofisticação das infrações virtuais, embora ainda limitadas em sua abrangência diante da mutabilidade tecnológica[67].

Apesar do avanço representado pela tipificação inicial, as referidas normas demonstram caráter reativo, pois surgiram de episódios midiáticos e não de um planejamento sistemático da política criminal digital. Essa característica pontual fez com que o ordenamento jurídico não acompanhasse, em tempo hábil, a complexidade dos crimes virtuais contemporâneos, que incluem fraudes financeiras, ransomware e ataques massivos de dados. Assim, a legislação penal brasileira carece de uma estrutura normativa coesa e preventiva[68].

Além de criminalizar a invasão de dispositivos, a Lei nº 12.737/2012 trouxe a necessidade de ordem judicial para obtenção de dados, o que reafirma o respeito ao devido processo legal. Contudo, a falta de detalhamento sobre os meios de investigação e coleta de provas digitais gera insegurança jurídica, especialmente quanto à integridade da cadeia de custódia. Nessa perspectiva, a legislação deve dialogar com o Código de Processo Penal, que em seus artigos 158-A a 158-F estabelece as diretrizes para o tratamento técnico das evidências digitais[69].

Outro ponto relevante é a interação entre a Lei Carolina Dieckmann e a Lei nº 9.296/1996, que regula as interceptações telefônicas e telemáticas. A compatibilização entre essas normas é indispensável, já que a captação de dados e comunicações eletrônicas é essencial para a investigação de crimes digitais. No entanto, a aplicação prática dessas medidas enfrenta desafios técnicos e éticos, especialmente no que se refere à proteção da intimidade e ao princípio da proporcionalidade[70].

A evolução dos crimes cibernéticos evidencia que o Direito Penal tradicional não consegue, sozinho, conter práticas tão dinâmicas e de alcance global. A Lei nº 12.737/2012, embora relevante, não abarca condutas mais sofisticadas, como manipulação de algoritmos e uso de inteligência artificial para fraudes. Isso reforça a necessidade de reformas legislativas contínuas, voltadas à atualização da tipificação penal e à integração com padrões internacionais[71].

---

[67] BRASIL, 2012, p. 1.
[68] MONTEL, Izadora Fonseca; DE PAIVA, Jaqueline de Kassia Ribeiro. CRIMES CIBERNÉTICOS: PANORAMA LEGISLATIVO. Revista Ibero-Americana de Humanidades, Ciências e Educação, v. 10, n. 11, p. 4495-4523, 2024. p. 4501.
[69] BRASIL, 2022, p. 1.
[70] BRASIL, 1996, p. 1.
[71] SOBRINHA, Ana Amélia Fernandes Albuquerque; MESSIAS, Marcos Venicius Nunes; TEMPONI, Pedro Henrique Araujo. RESPONSABILIZAÇÃO PENAL NOS CRIMES CIBERNÉTICOS: UM ESTUDO SOBRE A LEGISLAÇÃO BRASILEIRA E A SEGURANÇA JURÍDICA. Estudos de Direito Penal e Processo Penal na Contemporaneidade: 2a Edição, 2025. p. 22.

A abordagem constitucional também deve ser considerada, uma vez que o avanço da legislação penal sobre o ambiente digital deve respeitar os limites impostos pelo princípio da legalidade. Esse princípio exige precisão e clareza na definição dos tipos penais, evitando interpretações extensivas que comprometam a segurança jurídica. Assim, o legislador deve buscar equilíbrio entre inovação normativa e proteção de direitos fundamentais[72].

Outro desafio recorrente é a tensão entre liberdade de expressão e repressão penal. Crimes como difamação e discurso de ódio em plataformas digitais colocam em conflito o direito à manifestação e o dever do Estado de proteger a dignidade humana. A doutrina contemporânea aponta para a necessidade de critérios objetivos que diferenciem o exercício legítimo da opinião pública das práticas criminosas[73].

Do ponto de vista técnico-jurídico, a ausência de uniformidade na aplicação das Leis nº 12.737/2012 e nº 12.735/2012 contribui para interpretações divergentes entre tribunais. Tal cenário afeta a previsibilidade das decisões e compromete a efetividade da persecução penal. É essencial que o sistema de justiça desenvolva diretrizes unificadas de interpretação, baseadas na doutrina penal e no princípio da tipicidade estrita[74].

Essas leis inaugurais representam o primeiro passo na construção de uma política criminal voltada à proteção do espaço digital. Contudo, sua efetividade depende de constante atualização e de integração com novas tecnologias, garantindo que a lei acompanhe o ritmo das transformações sociais e tecnológicas. A criminalidade cibernética, ao desafiar fronteiras e categorias jurídicas tradicionais, exige um Direito Penal adaptável e tecnicamente informado[75].

O Marco Civil da Internet (Lei nº 12.965/2014) e a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) consolidam o arcabouço jurídico de proteção da privacidade e da segurança informacional no Brasil. O Marco Civil define princípios como a proteção da intimidade, da liberdade de expressão e da neutralidade da rede, estabelecendo regras claras para a guarda e o fornecimento de registros de conexão e de acesso mediante ordem judicial. Já a LGPD introduz parâmetros técnicos e jurídicos para o tratamento de dados pessoais, reforçando o direito fundamental à autodeterminação informativa e o dever de

---

[72] BARROSO, Luís Roberto. *Curso de direito constitucional contemporâneo: os conceitos fundamentais e a construção do novo modelo*. 7. ed. São Paulo: Saraiva Educação, 2018. ISBN 9788547230869 p. 231.
[73] DIAS, Júlia Gabrielly Freitas; DANTAS FILHO, Jerônimo Vieira. Cibercriminalidade: Os crimes cibernéticos e os limites da liberdade de expressão na internet. NATIVA-Revista de Ciências, Tecnologia e Inovação (ISSN: 2764-1295), v. 8, n. 2, p. 73-82, 2025. p. 78.
[74] TAVARES, Juarez. Projeto de Código Penal: a reforma da parte geral. *Revista da EMERJ*, v. 15, n. 60, p. 161-189, 2012. p. 172.
[75] BRASIL, 2012, p. 2.

responsabilização das instituições que manipulam dados sensíveis[76].

A preservação de registros digitais prevista no Marco Civil é essencial para a persecução penal, pois permite identificar o caminho percorrido por agentes que cometem crimes na rede. Essa obrigação imposta aos provedores, contudo, deve observar limites constitucionais, como o respeito ao sigilo das comunicações e à proporcionalidade no uso das informações coletadas. Assim, o equilíbrio entre investigação e privacidade torna-se o ponto central da aplicação prática da norma[77].

A LGPD, ao regulamentar o tratamento de dados pessoais, introduziu uma nova lógica de corresponsabilidade no ciberespaço. As instituições públicas e privadas que armazenam informações são obrigadas a adotar medidas preventivas e a comunicar incidentes de segurança, sob pena de sanções administrativas e civis. No contexto penal, essas disposições repercutem diretamente na coleta e preservação de provas digitais, garantindo que o processo ocorra dentro de parâmetros técnicos e éticos[78].

O diálogo entre o Marco Civil e a LGPD é indispensável para a aplicação equilibrada do direito penal digital. Enquanto o primeiro trata da infraestrutura da rede e da guarda de registros, o segundo regula o conteúdo e o ciclo de vida dos dados pessoais. Essa complementaridade assegura uma base normativa sólida para que o Estado investigue delitos cibernéticos sem violar garantias fundamentais, especialmente o direito à privacidade e à inviolabilidade de dados[79].

No entanto, a aplicação prática dessas leis enfrenta entraves técnicos e operacionais. A ausência de padronização entre provedores, a demora na resposta a ordens judiciais e as dificuldades na rastreabilidade de informações criptografadas ainda comprometem a eficácia investigativa. O avanço das técnicas de anonimização e do uso de VPNs desafia a efetividade do Marco Civil e evidencia a necessidade de atualização constante das normas[80].

Outro desafio surge na interface entre a proteção de dados e o princípio da legalidade penal. A coleta de informações sem autorização judicial, ainda que em nome da segurança, configura violação ao devido processo legal. O respeito à cadeia de custódia e aos procedimentos de obtenção da prova é essencial para evitar nulidades e garantir a validade do

---

[76] BRITO, 2017, p. 45.
[77] SOBRINHA; MESSIAS; TEMPONI, 2025, p. 103.
[78]SILVA, Fernanda Bílio et al. A tipificação das condutas praticadas em ambiente virtual. *NOVOS DIREITOS*, v. 10, n. 1, p. 74-88, 2023. p. 76.
[79]MAIA, Karolline Barbosa; COSTA, Cezar Henrique Ferreira. CRIMES CIBERNÉTICOS. Revista Ibero-Americana de Humanidades, Ciências e Educação, v. 9, n. 10, p. 109-126, 2023. p. 118.
[80] FRAGA, Bruno; VANGLLER, Thompson. *Técnicas de invasão*. Compilado a partir de videoaulas e pesquisas por Thompson Vangller; idealização do projeto por Bruno Fraga. Londres, 2017. p. 252.

processo. Assim, a LGPD reforça o dever estatal de agir com transparência e responsabilidade durante as investigações criminais[81].

A realidade mostra que muitas das violações de privacidade não decorrem de falhas técnicas, mas da manipulação psicológica de usuários, fenômeno amplamente descrito pela engenharia social. Como demonstram estudos clássicos, o elo mais vulnerável na segurança digital é o comportamento humano, o que torna indispensável a educação informacional como instrumento complementar às normas jurídicas[82].

O Marco Civil e a LGPD também impõem um novo paradigma de cooperação entre Estado e provedores de serviço, com o objetivo de garantir respostas rápidas e tecnicamente adequadas às demandas judiciais. Essa relação, porém, precisa de protocolos claros para evitar abusos e conflitos de competência. O compartilhamento de dados deve ser regido pela legalidade estrita, preservando a finalidade legítima e o princípio da minimização das informações coletadas[83].

A conjugação dessas duas leis demonstra a transição do Brasil para um modelo jurídico de governança digital, em que o respeito à privacidade não é obstáculo à persecução penal, mas condição para sua legitimidade. O fortalecimento desse equilíbrio entre segurança e liberdade é o caminho para a consolidação de uma cultura jurídica compatível com os desafios da era digital[84].

3.2 Projetos de lei e propostas de atualização normativa

O avanço das tecnologias digitais trouxe à tona a urgência de reformar o Código Penal Brasileiro, adequando-o às novas modalidades criminosas que surgem em ambientes virtuais e imersivos. Diversos projetos de lei tramitam atualmente no Congresso Nacional, com o objetivo de ampliar a cobertura penal para condutas praticadas em meios digitais, como fraudes em criptomoedas, deepfakes, crimes no metaverso e ataques cibernéticos transnacionais. Essas propostas buscam não apenas atualizar a legislação, mas também compatibilizar os princípios tradicionais da tipicidade e da legalidade com a realidade tecnológica contemporânea[85].

Um dos principais desafios enfrentados pelas reformas propostas está na delimitação precisa das condutas típicas. A volatilidade das práticas digitais exige que a lei adote uma

[81] BRASIL, 2012, p. 3.
[82] MITNICK; SIMON, 2003, p. 91.
[83] BRITO, 2017, p. 83.
[84] SOBRINHA; MESSIAS; TEMPONI, 2025, p. 109.
[85] SILVA et al., 2023, p. 77.

linguagem tecnológica neutra, capaz de abranger diferentes formas de ataque sem violar o princípio da taxatividade. A insegurança jurídica provocada pela ausência de parâmetros claros prejudica tanto a persecução penal quanto o direito de defesa. Por isso, os legisladores têm debatido a criação de categorias penais específicas voltadas ao ambiente virtual, como "crimes informáticos complexos" e "infrações digitais imersivas"[86].

As propostas de reforma também têm o objetivo de consolidar o entendimento sobre a responsabilidade penal em espaços virtuais. Com o surgimento do metaverso e de ambientes de realidade aumentada, surgem novas formas de interação que desafiam conceitos clássicos como autoria, dolo e materialidade. Determinar a consumação de um crime em um espaço digital exige revisão dos parâmetros jurídicos tradicionais, considerando que muitas condutas possuem efeitos simbólicos, mas geram danos concretos às vítimas[87].

Outro ponto central do debate legislativo é a ampliação da proteção de bens jurídicos digitais, como dados, identidades virtuais e ativos criptográficos. As propostas atuais buscam criminalizar o uso indevido de informações pessoais, a invasão de sistemas automatizados e o comércio ilegal de credenciais, fortalecendo a tutela penal do patrimônio informacional. Essa atualização é essencial para garantir a efetividade do direito penal diante da desmaterialização das relações econômicas e sociais[88].

Além disso, o Marco Civil da Internet permanece como instrumento fundamental de referência nas discussões sobre reforma penal, ao definir diretrizes para a preservação de registros e a cooperação entre provedores e autoridades. No entanto, especialistas alertam que o Marco Civil, de natureza principiológica, não substitui a necessidade de tipificações penais específicas. As propostas de atualização do Código Penal visam justamente complementar esse arcabouço, conferindo maior precisão às sanções aplicáveis às condutas ilícitas digitais[89].

As discussões legislativas também abordam o uso crescente da inteligência artificial em práticas criminosas, como a geração automatizada de desinformação, falsificação de imagens e manipulação de conteúdo. As reformas sugeridas incluem a criação de tipos penais específicos para o uso indevido de IA em prejuízo de terceiros, reconhecendo o impacto ético e jurídico dessas tecnologias. A falta de previsão expressa gera lacunas que comprometem a efetividade do sistema penal e dificultam a responsabilização dos agentes envolvidos[90].

---

[86] MAIA; COSTA, 2023, p. 114.
[87] SANTANA, 2021, p. 9.
[88] COSTA, 2021, p. 15.
[89] BRASIL, 2014, p. 2.
[90] CUNHA, Vinícius Ferreira; CORTIZO, Vitor Martins. CRIMES CIBERNÉTICOS: Implicações Legais, eficácia das leis existentes e necessidade de adaptação do sistema legal a era digital. Revista Acadêmica Online, v. 10, n. 51, p. 1-18, 2024. p. 8.

Outro aspecto relevante nas propostas de modernização é a ampliação da cooperação internacional. Como grande parte dos crimes cibernéticos possui natureza transnacional, a legislação brasileira precisa harmonizar-se com tratados e convenções globais, como a Convenção de Budapeste. A integração de mecanismos internacionais fortalece o combate a delitos praticados por redes descentralizadas e melhora a eficiência das investigações e da coleta de provas digitais[91].

A reforma do Código Penal deve, portanto, seguir diretrizes que conciliem segurança jurídica e inovação tecnológica. É indispensável que o legislador adote uma abordagem preventiva e adaptativa, criando dispositivos capazes de acompanhar as transformações digitais sem recorrer a cláusulas penais abertas. Isso implica investir em redação técnica, formação de especialistas em direito digital e diálogo com a comunidade científica[92].

As reformas em discussão representam um movimento de amadurecimento do sistema jurídico brasileiro frente à era digital. A modernização do Código Penal é condição necessária para assegurar a eficácia do princípio da legalidade e a tutela dos bens jurídicos no ciberespaço. No entanto, deve-se evitar o expansionismo punitivo, preservando os direitos fundamentais e a proporcionalidade das penas. O futuro do direito penal dependerá da capacidade de equilibrar repressão e garantismo em um contexto de inovação constante[93].

A ampliação da tipicidade penal diante da criminalidade cibernética impõe um desafio delicado ao legislador, pois qualquer inovação normativa deve respeitar os limites constitucionais da legalidade e da taxatividade. A criação de tipos penais abertos, com termos vagos ou indeterminados, pode violar a exigência de precisão normativa prevista no artigo 5º, inciso XXXIX, da Constituição Federal, gerando insegurança jurídica e abrindo espaço para arbitrariedades interpretativas. Assim, a modernização do Direito Penal deve ser conduzida com rigor técnico, evitando que a urgência em combater crimes digitais comprometa princípios fundamentais[94].

O princípio da legalidade penal estabelece que não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal. Essa regra, essencial ao Estado Democrático de Direito, impede que o poder punitivo seja exercido de forma arbitrária. No contexto digital, onde surgem condutas inéditas e complexas, cresce a tentação de criar leis amplas e genéricas

[91] HERNANDEZ, Erika Fernanda Tangerino; DE TOLEDO, Nathália Karina Abucci. Crimes cibernéticos: seus efeitos revolucionários diante de uma legislação em constante evolução. *Revista Jurídica da UniFil,* v. 17, n. 17, p. 72-84, 2021. p. 80.
[92] SILVA et al., 2023, p. 86.
[93] SANTANA, 2021, p. 11.
[94] COSTA, 2021, p. 13.

para abarcar novos comportamentos. Contudo, essa prática fere a taxatividade penal e coloca em risco a previsibilidade e a segurança do cidadão perante o Estado[95].

O debate sobre os limites constitucionais na tipificação de crimes tecnológicos está diretamente ligado à natureza mutável do ambiente digital. Novas formas de interação e comunicação surgem em ritmo acelerado, e a legislação não consegue acompanhá-las na mesma velocidade. A tentativa de criar dispositivos "abertos" para abranger futuras condutas, embora compreensível, pode levar ao afastamento dos fundamentos garantistas do Direito Penal. O resultado é um sistema normativo instável, sujeito a interpretações elásticas e decisões arbitrárias[96].

Outro ponto de atenção é a necessidade de compatibilizar o Direito Penal com o Marco Civil da Internet, especialmente no que diz respeito à responsabilidade dos provedores e à preservação de dados. A expansão desmedida dos tipos penais não pode transferir responsabilidades penais a entes privados sem o devido respaldo legal. A legislação deve diferenciar claramente as esferas civil, administrativa e penal, evitando sobreposição de deveres e punições indevidas[97].

A doutrina contemporânea defende que a precisão terminológica na redação das normas penais digitais é condição indispensável para preservar o princípio da culpabilidade. Em crimes cometidos no ciberespaço, o dolo e a materialidade são muitas vezes de difícil comprovação, e a vagueza na definição das condutas pode levar à punição de comportamentos neutros ou socialmente aceitáveis. Portanto, o legislador deve optar por uma tipificação objetiva e restrita, limitada a ações de comprovado dano social[98].

A ampliação da tipicidade penal também deve observar o princípio da proporcionalidade, evitando sanções desmedidas diante de condutas de baixo potencial ofensivo. No ambiente digital, onde o alcance e o impacto das ações podem ser amplificados artificialmente, é fundamental distinguir entre a gravidade real do dano e o simples risco potencial. A proteção de bens jurídicos deve continuar sendo o eixo orientador da intervenção penal, e não o clamor social por punições severas[99].

---

[95] CUNHA; CORTIZO, 2024, p. 4.
[96] HERNANDEZ; TOLEDO, 2021, p. 78.
[97] COLAÇO, Hian Silva. Liability of internet service providers: dialogue between the jurisprudence and the civil mark of internet. Revista dos Tribunais, v. 2017, p. 02-16, 2017. p. 11.
[98] OLIVEIRA, Mozart Gustavo Faria de. Repensando os tipos penais do crime permanente, crime instantâneo de efeito permanente e do crime continuado no âmbito da rede mundial de computadores e redes sociais. Qual a melhor forma de qualificação do stalking agora previsto no Art. 147 A do Código Penal Brasileiro? 2023. 71 f. Trabalho de Conclusão de Curso (Bacharelado em Direito) - Faculdade Nacional de Direito, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2023. p. 28.
[99] QUEIROZ, Liv Ferreira Augusto Severo. Os crimes cibernéticos no ordenamento jurídico brasileiro:

No cenário internacional, observa-se que países que adotaram legislações excessivamente abrangentes acabaram enfrentando problemas de legitimidade e de aplicação prática. O Brasil deve aprender com essas experiências e seguir um caminho de equilíbrio, privilegiando a técnica legislativa e o controle de constitucionalidade. O Direito Internacional Público também oferece parâmetros importantes, ao destacar que a criminalização deve respeitar os princípios universais de necessidade e proporcionalidade, assegurando a proteção simultânea da liberdade individual e da ordem jurídica[100].

A expansão da tipicidade penal sem base conceitual sólida pode gerar uma criminalização simbólica, em que a lei é criada apenas para demonstrar resposta estatal, sem eficácia prática. Essa prática, comum em temas de forte repercussão midiática, como o cibercrime, enfraquece o sistema jurídico e gera desconfiança na sociedade. É imprescindível que as reformas penais sejam precedidas de estudos técnicos e de impacto legislativo, garantindo coerência e aplicabilidade[101].

O desafio contemporâneo consiste em equilibrar inovação normativa e fidelidade aos princípios constitucionais. O Direito Penal não deve servir como instrumento de reação emocional, mas como mecanismo racional de proteção de bens jurídicos relevantes. A tipificação dos crimes cibernéticos deve ser clara, restrita e tecnicamente precisa, de modo que a lei não se torne uma ameaça à liberdade, mas um instrumento legítimo de segurança jurídica e justiça social[102].

3.3 Tratados e convenções internacionais sobre cibercrimes

A globalização das redes digitais exigiu que o combate ao cibercrime fosse tratado em escala internacional, levando à criação de convenções multilaterais que buscam harmonizar legislações e procedimentos de investigação. Entre as mais influentes estão as iniciativas da ONU, da OCDE e do Conselho da Europa, que estabeleceram padrões normativos e técnicos voltados à cooperação interestatal e à uniformização de conceitos jurídicos aplicáveis a delitos digitais. Essas convenções são fundamentais para reduzir a fragmentação normativa e garantir respostas coordenadas às ameaças globais[103].

investigação criminal e desafios. Revista do CNMP, n. 12, p. 417-448, 2024. p. 430.
[100] PORTELA, Paulo Henrique Gonçalves. Direito internacional público e privado. 2025. p. 90.
[101] FRUMI, Patrícia. Marco Civil da Internet, provedores de informação e responsabilidade civil por cyberbullying. Revista dos Tribunais, v. 1044, p. 145-167, 2022. p. 161.
[102] COSTA, 2021, p. 17.
[103] SOBRINHA; MESSIAS; TEMPONI, 2025, p. 57.

A Organização das Nações Unidas (ONU) tem papel pioneiro na formulação de diretrizes voltadas ao combate ao cibercrime. Desde os anos 1990, por meio do Escritório das Nações Unidas sobre Drogas e Crime (UNODC), a ONU promove conferências e relatórios que incentivam os países-membros a tipificar condutas como invasão de sistemas, fraude digital e disseminação de malware. Essas recomendações buscam equilibrar segurança e direitos humanos, assegurando que a expansão do controle estatal não viole liberdades fundamentais[104].

A OCDE (Organização para a Cooperação e Desenvolvimento Econômico) também desempenha papel relevante na construção de políticas internacionais de segurança cibernética. Sua contribuição principal está na definição de princípios de governança da internet e na elaboração de normas para proteção de dados pessoais e confidenciais. Esses instrumentos ajudam a prevenir crimes como espionagem corporativa e roubo de informações sigilosas, favorecendo um ambiente digital mais seguro e transparente entre os Estados-membros[105].

No âmbito europeu, a principal referência é a Convenção de Budapeste sobre Crimes Cibernéticos (2001), promovida pelo Conselho da Europa. Este tratado é o primeiro instrumento internacional vinculante sobre o tema, estabelecendo padrões mínimos para a criminalização de condutas informáticas e procedimentos processuais relacionados à obtenção e preservação de provas digitais. Sua importância transcende o continente europeu, pois foi ratificada por diversos países não europeus, incluindo o Brasil, que adota seus parâmetros como referência de boas práticas legislativas[106].

Além da Convenção de Budapeste, o Protocolo Adicional (CETS 189) ampliou a cooperação entre Estados no enfrentamento de crimes de ódio e discriminação praticados por meios eletrônicos. Esse instrumento reforça a necessidade de um vocabulário jurídico tecnológico neutro e de procedimentos ágeis para troca de informações entre autoridades. Tal flexibilidade é essencial diante da natureza dinâmica e transnacional dos crimes cibernéticos[107].

Outra vertente relevante está na influência das convenções internacionais sobre a legislação nacional. No Brasil, dispositivos como o Marco Civil da Internet e a Lei Geral de Proteção de Dados (LGPD) refletem diretrizes globais de proteção à privacidade, transparência e segurança digital. Essa convergência normativa fortalece o alinhamento do país às boas práticas internacionais e demonstra o papel dos tratados como instrumentos de modernização legislativa e proteção de direitos fundamentais[108].

---

[104] CUNHA; CORTIZO, 2024, p. 7.
[105] HERNANDEZ; TOLEDO, 2021, p. 80.
[106] QUEIROZ, 2024, p. 421.
[107] OLIVEIRA, 2023, p. 43.
[108] COLAÇO, 2017, p. 15.

A adesão a essas convenções também reforça o princípio da cooperação internacional em matéria penal, previsto em diversos diplomas jurídicos nacionais e internacionais. O Código de Processo Penal brasileiro, ao introduzir normas sobre cadeia de custódia e cooperação jurídica, busca garantir a validade das provas obtidas em investigações transnacionais. Esse alinhamento normativo amplia a capacidade do Estado em enfrentar delitos complexos que ultrapassam fronteiras físicas e jurisdicionais[109].

Contudo, a efetividade das convenções depende da implementação prática pelos Estados signatários. Muitos países ainda enfrentam dificuldades técnicas e estruturais para adotar padrões internacionais de rastreamento digital e proteção de dados. A falta de uniformidade legislativa dificulta a cooperação entre órgãos de persecução penal e cria zonas de impunidade cibernética, nas quais criminosos se aproveitam das lacunas jurídicas entre diferentes jurisdições[110].

A harmonização global da legislação penal em matéria de cibercrime deve ser entendida como um processo contínuo e adaptativo. A tecnologia evolui mais rapidamente que o direito, o que exige atualização constante das normas e dos mecanismos de cooperação. Nesse contexto, as convenções internacionais não apenas orientam a tipificação penal, mas também promovem o fortalecimento do Estado de Direito no ambiente digital, assegurando equilíbrio entre repressão, garantismo e soberania jurídica[111].

A cooperação jurídica internacional tornou-se um dos pilares centrais no enfrentamento dos crimes cibernéticos, dada a natureza transnacional das infrações digitais e a dispersão dos agentes e dos dados em múltiplas jurisdições. A integração entre Estados para o compartilhamento de informações e provas digitais é essencial para garantir a eficácia das investigações e a responsabilização dos autores. A ausência dessa cooperação compromete o alcance das investigações, uma vez que as fronteiras físicas se tornaram insuficientes para delimitar a atuação criminosa em rede[112].

A Convenção de Budapeste, ao estabelecer diretrizes internacionais para a cooperação penal em matéria de crimes cibernéticos, consolidou o entendimento de que o combate efetivo a tais delitos depende de mecanismos ágeis de intercâmbio de provas, preservação de registros e auxílio jurídico mútuo. Essa integração possibilita o rastreamento de transações e comunicações eletrônicas, além de garantir a autenticidade e a validade processual das

[109] BRASIL, 2020, p. 4.
[110] BARROSO, 2018, p. 92.
[111] TAVARES, 2012, p. 172.
[112] BRASIL, 2014, p. 2.

evidências colhidas em ambientes digitais[113].

No âmbito nacional, o Marco Civil da Internet e a Lei nº 12.737/2012 incorporam princípios compatíveis com os tratados internacionais, estabelecendo a obrigatoriedade de preservação de dados e a necessidade de cooperação entre provedores e autoridades judiciais. Essa harmonia normativa fortalece a atuação do Brasil como parte integrante da rede global de combate à criminalidade digital. A cooperação técnica entre o Judiciário e os provedores de serviços digitais é, nesse sentido, elemento indispensável para a eficiência investigativa[114].

Contudo, a obtenção e o compartilhamento de provas digitais ainda enfrentam desafios relacionados à soberania e à diversidade legislativa entre os países. A incompatibilidade de prazos de retenção de dados e de regras sobre proteção à privacidade gera entraves ao fluxo de informações. É preciso um equilíbrio entre a proteção de direitos fundamentais e a necessidade de celeridade nas investigações criminais. Essa tensão exige o aprimoramento de acordos bilaterais e multilaterais que padronizem procedimentos de cooperação jurídica[115].

Os MLATs (Mutual Legal Assistance Treaties), tratados de assistência jurídica mútua, são instrumentos essenciais nesse processo, pois viabilizam a troca formal de informações entre países, respeitando o devido processo legal e as garantias constitucionais. Embora esses mecanismos sejam eficazes, sua morosidade ainda representa um obstáculo à rápida identificação e responsabilização dos cibercriminosos. O fortalecimento de canais diretos de comunicação entre autoridades, como o uso de redes seguras de intercâmbio eletrônico, pode mitigar tais dificuldades[116].

A responsabilização penal transnacional também depende da cooperação técnica entre órgãos de persecução. O compartilhamento de perícias digitais, técnicas de rastreamento e protocolos de preservação da prova contribui para a integridade das investigações e evita a perda de evidências. Além disso, a capacitação de profissionais da justiça e da polícia em tecnologia forense é imprescindível para lidar com as complexidades do ambiente virtual e garantir a autenticidade das informações obtidas[117].

Autores da área da segurança digital, como Bruno Fraga, ressaltam que a cooperação internacional não deve limitar-se ao campo jurídico, mas estender-se à esfera tecnológica. O desenvolvimento de padrões comuns de criptografia, autenticação e monitoramento de ameaças

[113] COSTA, 2021, p. 9.
[114] CUNHA; CORTIZO, 2024, p. 5.
[115] HERNANDEZ; TOLEDO, 2021, p. 77.
[116] SOBRINHA; MESSIAS; TEMPONI, 2025, p. 68.
[117] BRITO, 2017, p. 120.

facilita a atuação conjunta entre países e empresas privadas, formando uma rede de defesa cibernética global. Tal integração reduz o tempo de resposta às investigações e impede que criminosos explorem lacunas geográficas para escapar da punição[118].

A cooperação também contribui para o fortalecimento da segurança jurídica internacional, permitindo que as decisões judiciais tenham maior alcance e que a execução penal seja efetivada mesmo em casos de múltiplas jurisdições. O diálogo entre os sistemas jurídicos nacionais e as cortes internacionais deve ser intensificado, especialmente diante de crimes que envolvem violações de direitos humanos e manipulação de dados sensíveis[119].

O avanço da cooperação jurídica internacional representa não apenas uma estratégia de combate ao cibercrime, mas também um movimento de consolidação do Estado de Direito no ambiente digital. Ao alinhar políticas penais, práticas forenses e princípios constitucionais, os países constroem um modelo global de governança jurídica que privilegia a justiça, a transparência e a proteção dos cidadãos frente às novas ameaças tecnológicas. A consolidação dessa estrutura é, portanto, um passo essencial para garantir a eficácia penal e a segurança digital no século XXI[120].

3.4 A Convenção de Budapeste e a cooperação internacional

A Convenção de Budapeste sobre Crimes Cibernéticos (CETS 185), firmada em 2001 pelo Conselho da Europa, é o principal instrumento jurídico internacional destinado à criminalização de condutas cibernéticas. Seu objetivo é promover a harmonização das legislações nacionais e fortalecer a cooperação internacional na investigação e persecução penal de delitos praticados por meios digitais. O tratado define categorias de crimes informáticos e estabelece diretrizes processuais compatíveis com os princípios do devido processo legal e da legalidade penal, garantindo que a inovação normativa não ultrapasse os limites constitucionais[121].

Entre as principais condutas tipificadas pela Convenção estão a acesso ilícito (art. 2º), a interceptação ilegal de comunicações (art. 3º), a interferência em dados e sistemas (arts. 4º e 5º) e o uso indevido de dispositivos tecnológicos (art. 6º). Essas disposições representam um marco na transposição de comportamentos tecnológicos em tipos penais claros e objetivos. O texto

[118] FRAGA; VANGLLER, 2017, p. 314.
[119] COLAÇO, 2017, p. 13.
[120] BARROSO, 2018, p. 101.
[121] CONSELHO DA EUROPA, 2001, p. 5.

procura equilibrar a repressão criminal e a preservação das liberdades civis, evitando a criação de normas de caráter aberto ou genérico que possam violar o princípio da taxatividade penal[122].

A Convenção também se destaca pela abordagem processual inovadora, ao prever instrumentos específicos para preservação rápida de dados armazenados e produção de provas eletrônicas (arts. 16 a 21). Tais mecanismos asseguram que informações voláteis — como registros de IP ou logs de acesso — possam ser retidas e analisadas sem comprometer o devido processo. Esses dispositivos foram posteriormente incorporados em legislações nacionais, como o Marco Civil da Internet e o Código de Processo Penal brasileiro, fortalecendo a integridade das provas digitais[123].

Outro aspecto relevante é a compatibilidade da Convenção com o princípio da legalidade penal, uma vez que suas tipificações são redigidas em linguagem tecnológica neutra, permitindo que as normas se adaptem à evolução dos meios digitais sem necessidade de alterações constantes. Essa característica garante que a norma seja previsível e aplicável, evitando lacunas interpretativas que comprometam a segurança jurídica e a legitimidade da punição estatal[124].

No tocante à cooperação internacional, o tratado estabelece um modelo procedimental padronizado de auxílio mútuo entre autoridades de diferentes países. Esse modelo inclui a troca de informações sobre crimes em andamento, a execução de mandados de busca eletrônica e a assistência na coleta de provas digitais, sempre com respeito às legislações internas e aos princípios de soberania. Essa coordenação é essencial para combater a transnacionalidade típica dos crimes cibernéticos[125].

Do ponto de vista dogmático, a Convenção reforça a necessidade de que a legislação nacional mantenha um nexo de tipicidade estrita com os bens jurídicos tutelados. Isso significa que apenas condutas que efetivamente ameacem a integridade de sistemas e informações devem ser consideradas criminosas, afastando interpretações extensivas. Essa abordagem garantista dialoga diretamente com as ideias defendidas por Juarez Tavares, segundo as quais a criminalização deve ser um instrumento de proteção e não de expansão arbitrária do poder punitivo[126].

Além disso, o tratado prevê salvaguardas à liberdade de expressão e à privacidade,

[122] COSTA, 2021, p. 11.
[123] BRASIL, 2020, p. 3.
[124] CUNHA; CORTIZO, 2024, p. 8.
[125] HERNANDEZ; TOLEDO, 2021, p. 76.
[126] TAVARES, 2012, p. 170.

assegurando que as medidas de vigilância e interceptação sejam aplicadas sob controle judicial rigoroso. Essa preocupação é destacada pela doutrina contemporânea, que ressalta a importância de equilibrar segurança digital e direitos fundamentais. O texto de Dias e Dantas Filho exemplifica essa tensão ao discutir os limites da liberdade de expressão em ambientes virtuais sujeitos à regulação penal[127].

A aplicação prática da Convenção também evidencia desafios, especialmente na harmonização dos conceitos de autoria, tentativa e dolo em crimes cometidos por meio de redes distribuídas. O anonimato e a descentralização tecnológica dificultam a subsunção de condutas aos tipos previstos, exigindo uma adaptação constante dos mecanismos de investigação. O fortalecimento da cadeia de custódia da prova digital, previsto no ordenamento brasileiro, é uma resposta direta a essas dificuldades, garantindo autenticidade e rastreabilidade das evidências[128].

A Convenção de Budapeste consolidou-se como paradigma internacional para o Direito Penal informático, ao articular tipificação, cooperação e garantismo jurídico em um único instrumento. Sua influência ultrapassa o campo penal e alcança políticas públicas de segurança digital, promovendo uma visão integrada entre tecnologia e justiça. A compatibilidade com os princípios constitucionais de legalidade e proporcionalidade reforça sua legitimidade como modelo normativo, tornando-a referência obrigatória para os países que buscam modernizar suas legislações sem sacrificar os direitos fundamentais[129].

A cooperação internacional no combate aos crimes cibernéticos é um pilar essencial para a efetividade da persecução penal, considerando que as condutas virtuais frequentemente ultrapassam fronteiras físicas e jurídicas. Nesse cenário, os instrumentos de assistência mútua (MLATs) se tornaram mecanismos indispensáveis para a troca de informações, coleta de provas e cumprimento de ordens judiciais entre países. O objetivo é assegurar uma resposta coordenada às infrações digitais, respeitando ao mesmo tempo os princípios da soberania e da legalidade penal[130].

A Convenção de Budapeste (CETS 185) e o Protocolo Adicional (CETS 189) estabeleceram as bases jurídicas dessa cooperação, prevendo diretrizes para preservação e compartilhamento de dados eletrônicos entre Estados signatários. Essas normas permitem que as autoridades solicitem informações de provedores estrangeiros ou executem medidas

[127] DIAS; DANTAS FILHO, 2025, p. 75.
[128] BRASIL, 2020, p. 6.
[129] COLAÇO, 2017, p. 14.
[130] CONSELHO DA EUROPA, 2001, p. 8.

cautelares de apreensão digital em tempo hábil, garantindo a integridade da prova. A adesão a tais mecanismos representa um avanço significativo para a persecução penal internacional[131].

No entanto, o uso efetivo dos MLATs ainda enfrenta entraves burocráticos e temporais, especialmente em países de tradição jurídica diversa. A lentidão na tramitação de pedidos, somada à ausência de procedimentos eletrônicos padronizados, compromete a agilidade necessária às investigações digitais, onde a volatilidade das provas é um obstáculo constante. Essa defasagem entre a norma e a prática revela a necessidade de revisões estruturais nos canais de cooperação[132].

O Brasil, como país em desenvolvimento e de grande presença digital, vem adaptando seu sistema jurídico aos padrões do Conselho da Europa, incorporando instrumentos processuais compatíveis com os tratados internacionais. A criação de protocolos de cadeia de custódia da prova digital, previstos no Código de Processo Penal, é um exemplo dessa adequação. Essa medida assegura a validade das provas compartilhadas, reforçando o alinhamento com os parâmetros da Convenção de Budapeste[133].

Entretanto, a aplicação prática desses mecanismos esbarra em desafios ligados à soberania digital, uma vez que o compartilhamento de dados pode gerar conflitos entre jurisdições e leis de proteção de privacidade. A harmonização entre legislações internas e internacionais é fundamental para evitar violações de direitos fundamentais e assegurar a legalidade da cooperação. Essa tensão é constantemente debatida na doutrina contemporânea e requer prudência legislativa e diplomática [134].

Outro desafio está na disparidade tecnológica e institucional entre os países cooperantes. Enquanto nações europeias possuem infraestrutura consolidada para a investigação de crimes cibernéticos, países latino-americanos ainda carecem de sistemas integrados de monitoramento e comunicação. Essa assimetria cria uma dependência operacional que pode fragilizar a eficácia das investigações multilaterais e o equilíbrio da cooperação[135].

A doutrina aponta ainda que a ausência de padrões unificados de tipificação penal dificulta a cooperação, uma vez que determinados comportamentos podem não ser considerados crime em alguns ordenamentos. Essa divergência prejudica a aplicação do princípio da dupla incriminação, exigido para o cumprimento de pedidos internacionais de

[131] CONSELHO DA EUROPA, 2003, p. 11.
[132] HERNANDEZ; TOLEDO, 2021, p. 81.
[133] BRASIL, 2020, p. 5.
[134] PORTELA, 2025, p. 72.
[135] CUNHA; CORTIZO, 2024, p. 10.

assistência. É necessário, portanto, um esforço global para harmonizar os conceitos jurídicos ligados ao cibercrime[136].

Fortalecer a cooperação técnica e pericial entre os países signatários, priorizando o treinamento conjunto e o intercâmbio de especialistas em informática forense. Essa colaboração interdisciplinar permite o desenvolvimento de métodos de rastreamento digital mais eficazes e de protocolos que assegurem a autenticidade das provas digitais em processos judiciais transnacionais[137] [138].

A construção de uma política global de enfrentamento ao cibercrime exige não apenas acordos multilaterais, mas uma integração ética e jurídica pautada na proteção da dignidade humana e na segurança digital. A consolidação desses mecanismos simboliza o amadurecimento do Direito Penal internacional frente à complexidade dos crimes cibernéticos contemporâneos[139].

[136] COSTA, 2021, p. 12.
[137] QUEIROZ, 2024, p. 430
[138] OLIVEIRA, 2023, p. 59.
[139] DIAS; DANTAS FILHO, 2025, p. 79.

4 O princípio da legalidade e o direito penal digital

O princípio da legalidade constitui um dos pilares fundamentais do Direito Penal em um Estado Democrático de Direito, funcionando como limite intransponível ao exercício do poder punitivo estatal. Consagrado no artigo 5º, inciso XXXIX, da Constituição Federal, esse princípio estabelece que não há crime nem pena sem lei anterior que os defina, assegurando previsibilidade normativa, segurança jurídica e proteção contra arbitrariedades. No âmbito da dogmática penal, a legalidade se desdobra em exigências como a reserva legal, a anterioridade, a taxatividade e a vedação da analogia in malam partem, elementos essenciais para garantir que a intervenção penal se mantenha excepcional, racional e estritamente vinculada à proteção de bens jurídicos relevantes. Esses fundamentos assumem especial importância em contextos de rápida transformação social, nos quais cresce a pressão por respostas penais imediatas e, por vezes, pouco refletidas.

A emergência do chamado Direito Penal Digital tensiona de forma significativa os contornos tradicionais do princípio da legalidade, na medida em que os crimes cibernéticos se desenvolvem em ambientes virtuais marcados pela fluidez, pela desmaterialização das condutas e pela constante inovação tecnológica. A dificuldade de enquadrar práticas digitais complexas em tipos penais concebidos para a realidade física suscita debates sobre a suficiência das normas existentes, a necessidade de criação de novos tipos penais e os riscos de expansão indevida da tipicidade. Nesse cenário, o desafio central consiste em compatibilizar a atualização normativa com a preservação das garantias constitucionais penais, evitando tanto a omissão legislativa, que favorece a impunidade, quanto o excesso punitivo, que compromete a segurança jurídica. Assim, a análise do princípio da legalidade no contexto do direito penal digital revela-se essencial para compreender os limites e as possibilidades de uma atuação penal legítima frente às novas formas de criminalidade na era da informação.

4.1 O princípio da legalidade e a tipicidade penal em ambiente virtual

O princípio da legalidade, consagrado no artigo 5º, inciso XXXIX, da Constituição Federal, estabelece que não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal. Essa norma representa o alicerce do Estado Democrático de Direito e assegura que o poder punitivo estatal se mantenha dentro dos limites fixados pelo legislador, impedindo arbitrariedades interpretativas. No contexto digital, esse princípio ganha relevância ainda maior, pois a velocidade das transformações tecnológicas supera a capacidade de resposta normativa, exigindo um esforço hermenêutico constante para garantir que novas condutas sejam enquadradas sem ferir a reserva legal[140]

A função garantista da legalidade manifesta-se na previsibilidade e na segurança jurídica, que protegem o indivíduo de sanções arbitrárias. Em ambientes digitais, onde condutas como invasão de sistemas, disseminação de dados e manipulação de informações emergem com novas roupagens, o risco de ampliação interpretativa é elevado. A tipicidade penal, nesse cenário, deve servir como instrumento de contenção, preservando a legitimidade do Direito Penal e evitando que ele se torne um mecanismo de controle desmedido sobre a vida digital dos cidadãos[141]

O avanço das tecnologias de informação impôs ao legislador o desafio de adaptar o ordenamento jurídico a práticas que não possuem correspondência direta com tipos penais tradicionais. O princípio da reserva legal impede que lacunas sejam supridas por analogia ou extensões interpretativas que desvirtuem o caráter taxativo da norma penal. Essa garantia torna-se indispensável frente a crimes cibernéticos em constante evolução, exigindo precisão na definição das condutas e clareza quanto à sua materialidade[142]

A tipicidade penal, como expressão concreta da legalidade, desempenha papel essencial na determinação do que constitui um crime digital. Nos delitos informáticos, é fundamental que o núcleo da conduta seja bem delineado, sob pena de violação dos princípios constitucionais. A ausência de clareza pode gerar insegurança tanto para o julgador quanto para o cidadão comum, que deve ser capaz de compreender, de forma inequívoca, o que é ou não proibido. Essa previsibilidade é condição indispensável à legitimidade da pena[143]

---

[140] TAVARES, 2012, p. 168.
[141] BARROSO, 2018, p. 217.
[142] BRITO, 2017, p. 45.
[143] SANTANA, 2021, p. 4.

Entretanto, a inovação criminosa desafia a rigidez da lei penal. Condutas como o cyberstalking, o phishing e o uso de deepfakes surgem em ambientes digitais onde as fronteiras entre lícito e ilícito se tornam difusas. A reserva legal, nesse contexto, atua como baliza que impede que a interpretação judicial substitua a função legislativa, reforçando o papel do Congresso Nacional como único competente para criar tipos penais[144]

A legalidade, além de limitar o poder punitivo, tem também uma dimensão emancipatória: protege o cidadão da insegurança jurídica e da moralização do Direito Penal. Essa função ganha destaque diante da tendência contemporânea de criminalizar novas condutas em resposta a pressões sociais. No ambiente digital, o clamor por punições rápidas pode comprometer a racionalidade legislativa e o equilíbrio entre repressão e liberdade[145]

O princípio da legalidade, ao impedir punições retroativas ou criadas por analogia, reforça a confiança no sistema jurídico. Ele exige que o Estado defina previamente os limites da intervenção penal e assegure que a aplicação da norma se mantenha proporcional e necessária. No universo digital, isso significa resistir à tentação de criar leis emergenciais que, embora bem-intencionadas, podem restringir direitos fundamentais e comprometer a coerência dogmática do sistema[146]

A doutrina penal contemporânea destaca que o garantismo penal não é obstáculo à efetividade, mas condição para uma aplicação justa do Direito. A reserva legal atua como salvaguarda contra o expansionismo punitivo, garantindo que o combate ao crime digital se desenvolva de maneira compatível com os valores constitucionais. Assim, a tipicidade penal deve ser compreendida como ferramenta de equilíbrio entre proteção social e preservação das liberdades individuais[147]

Autores como Wermuth e Callegari evidenciam que a legalidade deve ser interpretada em consonância com os desafios tecnológicos, sem perder sua essência garantista. Nos crimes de cyberstalking, por exemplo, a definição legal do tipo penal exige precisão terminológica que evite confusões com condutas meramente incômodas. Essa postura reafirma que o princípio da legalidade não é um entrave, mas um guia para a construção de um Direito Penal digital coerente, previsível e constitucionalmente legítimo[148].

A dificuldade de subsunção das novas condutas tecnológicas ao Direito Penal

---

[144] COSTA, 2021, p. 8.
[145] BARROSO, 2018, p. 220.
[146] TAVARES, 2012, p. 170.
[147] SILVA et al., 2023, p. 80.
[148] WERMUTH, M. A. D.; CALLEGARI, André Luís. Stalking e cyberstalking: considerações críticas sobre o delito tipificado no art. 147-a do Código Penal brasileiro. Revista Brasileira de Ciências Criminais, v. 186, n. 2021, p. 105-126, 2021. p. 112.

tradicional revela uma das maiores fragilidades do sistema jurídico contemporâneo. O ordenamento brasileiro, moldado em uma era analógica, enfrenta desafios para enquadrar comportamentos digitais que surgem em velocidade exponencial. Práticas como o *phishing*, o *ransomware* e a criação de *deepfakes* não encontram correspondência imediata nos tipos penais clássicos, o que gera insegurança jurídica e risco de violação ao princípio da legalidade, que exige precisão e anterioridade na definição de crimes e penas[149]

O *phishing*, caracterizado pela indução fraudulenta de vítimas para obtenção de dados sensíveis, exemplifica uma conduta híbrida, que transita entre o estelionato e o furto qualificado por meio eletrônico. Contudo, sua natureza digital complexa — envolvendo engenharia social, uso de e-mails falsos e páginas clonadas — dificulta a subsunção direta a dispositivos existentes. A ausência de tipificação específica cria margens interpretativas amplas, que podem resultar em decisões contraditórias e inseguras no âmbito judicial[150].

O ransomware, por sua vez, representa uma evolução criminosa de natureza transnacional, em que dados são sequestrados digitalmente e liberados apenas mediante pagamento de resgate, normalmente em criptomoedas. Essa prática desafia o conceito clássico de extorsão, pois o objeto do crime não é físico, mas sim informacional. A impossibilidade de aplicar integralmente tipos penais tradicionais expõe a defasagem normativa e exige uma reformulação conceitual do que se entende por bem jurídico protegido na sociedade da informação[151].

As *deepfakes*, vídeos ou áudios falsificados com uso de inteligência artificial, representam uma ameaça inédita ao direito à imagem, à honra e até mesmo à segurança nacional. A manipulação hiper-realista de conteúdo digital cria uma zona cinzenta entre liberdade de expressão e fraude, tornando insuficiente o enquadramento pelos crimes de calúnia, difamação ou falsidade ideológica. A ausência de legislação específica sobre o uso criminoso de inteligência artificial amplia as brechas para impunidade e desafia a dogmática penal a redefinir seus limites[152]

O problema central está na defasagem estrutural entre a evolução tecnológica e o ritmo do processo legislativo. Enquanto os crimes digitais se sofisticam diariamente, o legislador

[149] HERNANDEZ; TOLEDO, 2021, p. 74.
[150]GUERRA, Mayelli; CANDEIA, Sarajane Rodrigues. A aplicação do crime de “estupro virtual” frente ao ordenamento jurídico brasileiro: análise segundo o princípio da legalidade. A revisão linguística é de responsabilidade dos autores., 2022. p. 19
[151] MERLONE, Nicholas Maciel. Breve introdução ao direito penal e criminologia crítica econômica e digital: uma nova abordagem. Revista OWL (OWL Journal)-REVISTA INTERDISCIPLINAR DE ENSINO E EDUCAÇÃO, v. 3, n. 3, p. 1-39, 2025.
[152] HERNANDEZ; TOLEDO, 2021, p. 80.

opera em ciclos longos e reativos, resultando em um ordenamento fragmentado e incapaz de oferecer respostas imediatas. Essa lacuna cria tensão entre o dever de punir e o respeito ao princípio da legalidade, que proíbe punições sem previsão legal anterior e taxativa[153]

Adicionalmente, a natureza globalizada da internet amplia o problema da subsunção penal, pois condutas ilícitas podem ser praticadas em um país e gerar efeitos em outro. A jurisdição e a territorialidade tornam-se conceitos fluídos, desafiando a aplicação dos princípios tradicionais de soberania. Nesse sentido, a legislação nacional precisa dialogar com normas internacionais para que a tipificação penal digital seja eficaz e juridicamente sustentável[154]

A ausência de correspondência entre tipos penais clássicos e comportamentos digitais reflete não apenas uma lacuna legislativa, mas também dogmática. A teoria do delito, construída a partir da materialidade física das ações humanas, precisa ser reinterpretada diante de práticas que se dão em meio virtual, sem contato direto com o bem jurídico. Crimes como o cyberstalking, o *hacking e o spoofing* desafiam categorias tradicionais como autoria, dolo e consumação, exigindo um novo olhar sobre a tipicidade e a culpabilidade[155]

Esse descompasso teórico leva parte da doutrina a propor uma revisão da dogmática penal, especialmente no que se refere à proteção de bens jurídicos informacionais. O Direito Penal, historicamente voltado à tutela da integridade física e patrimonial, precisa reconhecer a informação como novo núcleo de valor social. A reformulação conceitual do delito e da tipicidade é, portanto, condição para que o sistema jurídico acompanhe as transformações impostas pela era digital[156]

A dificuldade de subsunção das novas condutas tecnológicas revela a necessidade urgente de um Direito Penal digital coerente, fundado em princípios constitucionais e em uma dogmática adaptada à complexidade informacional. A superação desse desafio depende da integração entre juristas, técnicos e legisladores, a fim de formular normas capazes de equilibrar a eficácia punitiva com as garantias fundamentais. Somente assim será possível preservar a legitimidade do sistema penal em um cenário de constante inovação tecnológica[157]

4.2 O papel da taxatividade e da anterioridade no ciberespaço

A taxatividade penal é uma das manifestações mais relevantes do princípio da legalidade

[153] PORTELA, 2025, p. 233.
[154] COLAÇO, 2017, p. 11.
[155] OLIVEIRA, 2023, p. 25.
[156] MERLONE, 2025, p. 21.
[157] PORTELA, 2025, p. 236.

e atua como garantia essencial da segurança jurídica. Por meio dela, assegura-se que o cidadão tenha plena ciência das condutas proibidas e das sanções aplicáveis, impedindo interpretações extensivas e decisões arbitrárias por parte do Estado. No contexto digital, onde novas formas de criminalidade surgem com frequência, a exigência de tipos penais claros e precisos torna-se ainda mais indispensável para preservar a previsibilidade e a legitimidade do sistema penal[158]

A imprecisão legislativa em torno dos crimes informáticos tem levado à aplicação analógica de tipos penais tradicionais, prática que afronta a taxatividade e o próprio Estado de Direito. A ausência de definições técnicas e de limites conceituais adequados abre margem para punições baseadas em juízos morais ou pressões sociais, o que compromete a coerência dogmática do Direito Penal. Assim, garantir a clareza terminológica dos tipos penais é essencial para que o poder punitivo estatal se mantenha sob controle[159]

A taxatividade, portanto, é mais do que uma exigência técnica; é uma condição ética do Direito Penal democrático. Quando aplicada ao campo dos crimes informáticos, ela impede que comportamentos socialmente reprováveis, mas não juridicamente tipificados, sejam tratados como delitos. Isso assegura que apenas condutas previamente definidas pelo legislador possam gerar consequências penais, fortalecendo a segurança jurídica e a confiança dos cidadãos no sistema judicial[160]

No ambiente virtual, condutas como o *cyberstalking, o phishing* e o vazamento de dados pessoais evidenciam a importância de uma redação legislativa precisa. Muitas dessas práticas ainda carecem de delimitação objetiva, o que leva à dificuldade de enquadramento penal e ao risco de decisões contraditórias. Essa incerteza reforça a necessidade de que o legislador adote parâmetros técnicos e científicos ao redigir novos tipos penais voltados à criminalidade digital[161]

O fenômeno das *deepfakes* também ilustra o desafio contemporâneo da taxatividade. A manipulação digital de imagens e vídeos pode violar direitos fundamentais sem que haja previsão legal específica que enquadre essa conduta como criminosa. A lacuna normativa compromete o princípio da segurança jurídica e favorece tanto a impunidade quanto o uso abusivo da interpretação judicial. É imprescindível que as leis penais sejam redigidas com rigor técnico, garantindo a neutralidade e a precisão exigidas pela taxatividade[162].

---

[158] PORTELA, 2025, p. 236.
[159] MERLONE, 2025, p. 8.
[160] PORTELA, 2025, p. 147.
[161] MOTA, 2020, p. 112.
[162] ALVES, Bruno Moraes et al. Análise da responsabilização criminal dos criadores e propagadores de "deep fakes" no ordenamento jurídico brasileiro. Caderno Pedagógico, v. 21, n. 6, p. e4348-e4348, 2024. p. 5.

A ausência de tipos penais claros também repercute na responsabilidade das plataformas digitais e dos provedores de serviços de internet. O Marco Civil da Internet e a Lei Geral de Proteção de Dados estabeleceram bases civis e administrativas, mas o campo penal ainda carece de regulamentação precisa quanto à culpa e à omissão desses agentes. A falta de definição normativa quanto aos deveres de vigilância e cooperação gera insegurança jurídica e dificulta a efetiva responsabilização em casos de crimes virtuais[163]

A doutrina penal contemporânea destaca que a violação da taxatividade conduz a um perigoso expansionismo punitivo, no qual o Direito Penal passa a abarcar comportamentos ambíguos e moralmente controversos. No contexto digital, isso se traduz na tentativa de criminalizar ações tecnológicas sem respaldo científico ou sem avaliação adequada de suas consequências jurídicas. A clareza dos tipos penais é, portanto, um freio contra o arbítrio e uma salvaguarda da racionalidade jurídica[164]

Além de limitar o arbítrio judicial, a taxatividade tem papel educativo, pois orienta o comportamento social e fornece previsibilidade sobre o alcance das normas penais. Em crimes cibernéticos, essa função didática é essencial, já que o cidadão comum precisa compreender, de forma inequívoca, quais ações são proibidas no ambiente virtual. A obscuridade das normas, por outro lado, fomenta a insegurança e enfraquece o poder dissuasório do Direito Penal[165].

A manutenção da segurança jurídica depende de um equilíbrio entre inovação legislativa e fidelidade aos princípios constitucionais. O avanço tecnológico não pode justificar a criação de tipos penais abertos ou indeterminados, sob pena de retrocesso no campo das garantias fundamentais. A taxatividade deve ser preservada como núcleo estruturante da legalidade penal, assegurando que o combate aos crimes informáticos se desenvolva dentro dos limites democráticos do Direito[166]

O princípio da anterioridade penal estabelece que nenhuma lei penal pode retroagir para prejudicar o réu, sendo aplicável apenas a condutas praticadas após sua vigência. No contexto das novas tecnologias, esse princípio adquire relevância singular, pois os avanços digitais frequentemente criam comportamentos delituosos antes de sua previsão legal. A inovação tecnológica, por ocorrer em ritmo muito mais acelerado que o processo legislativo, provoca situações em que o Direito Penal se torna reativo, gerando zonas de impunidade ou

[163] FRUMI, 2022, p. 150.
[164] MERLONE, 2025, p. 18.
[165] GOMES, Luis Gustavo Cruz. Princípio da legalidade penal e jogos online. 2024. p. 32
[166] PORTELA, 2025, p. 150.

interpretações extensivas que desafiam a legalidade[167].

A anterioridade, enquanto garantia fundamental, impede que cidadãos sejam punidos por atos que não eram considerados crimes no momento de sua prática. Em meio digital, esse princípio é constantemente tensionado, uma vez que crimes como *phishing, ransomware e deepfake* surgiram antes de qualquer regulamentação específica. A ausência de previsão normativa imediata obriga o sistema jurídico a lidar com um vácuo temporal entre a ocorrência do fato e a criação da lei, comprometendo a efetividade da persecução penal e o respeito às garantias constitucionais[168].

A inovação tecnológica também influencia o tempo de validade das normas penais, pois leis que tratam de crimes digitais tendem a se tornar obsoletas rapidamente. O ciclo de vida das tecnologias é curto, e condutas criminosas evoluem junto com as ferramentas digitais. Assim, o princípio da anterioridade enfrenta o desafio de adaptar-se a um ambiente dinâmico, em que a atualização legislativa deve ser constante para evitar o esvaziamento da norma penal[169].

Por outro lado, o princípio da retroatividade benéfica, previsto no artigo 5º, inciso XL, da Constituição Federal, ganha importância nas situações em que novas leis tornam mais brandas as punições ou descriminalizam condutas. Em delitos digitais, essa possibilidade é recorrente, pois o legislador, ao ajustar a tipificação de um crime ou ao redefinir seus elementos, pode acabar beneficiando o réu. Esse fenômeno demonstra que o avanço tecnológico não apenas cria novas formas de criminalidade, mas também exige revisões humanizadoras da resposta penal[170].

A aplicação do princípio da anterioridade penal às condutas tecnológicas demanda equilíbrio entre segurança jurídica e adaptabilidade normativa. Se, por um lado, a lei deve ser anterior ao fato, por outro, o Direito Penal não pode se manter estático diante da constante transformação digital. O desafio é construir dispositivos suficientemente precisos e abrangentes para abranger inovações futuras sem recorrer a tipos penais abertos ou genéricos, que feririam a taxatividade[171].

---

[167] BARBOSA, Luana Cristhine Oliveira; CEZAR, André Althmann; CARVALHO, Thomaz Jefferson. A evolução do direito penal frente às novas tecnologias e o crime de estupro virtual. *Anais Eletrônico* ISBN 978-65-5615-164-9 X Mostra Interna de Trabalhos de Iniciação Científica III Mostra Interna de Trabalhos de Iniciação em Desenvolvimento Tecnológico e Inovação. 2024. p. 3

[168] BOTELHO, Daniela Garcia et al. 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. p. 2715

[169] SOUZA; CERVINSKI, 2021, p. 5.

[170] DORIGON, Tais Ross. Crimes digitais: o crime de estupro virtual e sua interpretação à luz do princípio da legalidade. 2024. p. 12.

[171] GABRIEL, Anderson De Paiva. O pragmatismo como paradigma do Direito Processual Penal

O fenômeno da engenharia social, amplamente explorado por criminosos cibernéticos, exemplifica a dificuldade de enquadrar práticas novas em normas existentes. Muitos ataques baseiam-se na manipulação psicológica de usuários, algo que escapa às estruturas clássicas do tipo penal. A ausência de previsão legal direta, aliada à necessidade de respeito à anterioridade, impede que tais condutas sejam punidas sem a devida tipificação, revelando a defasagem entre realidade tecnológica e legislação penal[172].

A doutrina moderna reconhece que o princípio da anterioridade penal não deve ser visto como obstáculo, mas como instrumento de racionalidade. Ele impede que o Direito Penal se torne um campo de improvisos interpretativos e garante que qualquer inovação normativa passe pelo devido processo legislativo. Essa precaução é essencial diante do poder das tecnologias de informação, que tendem a ampliar a vigilância e o controle estatal sobre os cidadãos, exigindo freios constitucionais firmes[173] .

Outro ponto relevante é o papel da jurisprudência na aplicação desse princípio a delitos tecnológicos. Embora o Judiciário tenha a função de interpretar a lei, sua atuação encontra limites intransponíveis na legalidade e na anterioridade. A tentativa de suprir lacunas por meio de decisões criativas pode gerar insegurança jurídica e abrir precedentes para a punição de condutas sem respaldo normativo, o que seria incompatível com os fundamentos do Estado de Direito[174]

O princípio da anterioridade penal reafirma que a inovação legislativa deve acompanhar a inovação tecnológica, sem ceder à tentação do punitivismo emergencial. A criminalização de novas condutas digitais deve ocorrer de forma criteriosa, precedida de debates técnicos e jurídicos que assegurem clareza, proporcionalidade e justiça. A preservação dessa garantia constitucional é, portanto, o que diferencia o Direito Penal democrático de respostas legislativas precipitadas frente à complexidade do ciberespaço[175]

4.3 Limites da lei penal tradicional diante de condutas digitais

A estrutura clássica da tipificação penal foi concebida em um contexto social e

contemporâneo. Tecnologia, consenso e whistleblowing. Londrina: Thoth Editora, 2022. p. 66.
[172] COSTA, Luís Gustavo Silva; CRUZ, Sarah Aparecida da. A engenharia social e os desafios da segurança da informação nas empresas. In: II Congresso Internacional do Grupo Unis. Fundação de Ensino e Pesquisa do Sul de Minas, 2016. p. 10.
[173] MITNICK; SIMON, 2003, p. 45.
[174] BOTELHO et al., 2023, p. 2720.
[175] BARBOSA; CEZAR; CARVALHO, 2024, p. 5.

tecnológico profundamente diferente do atual, no qual as relações criminosas ocorriam em ambiente físico e sob controle humano direto. No entanto, a emergência das redes descentralizadas, da automação e da inteligência artificial transformou radicalmente as formas de execução de delitos, gerando incertezas sobre a autoria, o dolo e o momento da consumação. Essa dissonância evidencia que os conceitos tradicionais de responsabilidade penal precisam ser reinterpretados à luz da complexidade do ciberespaço[176]

Em crimes praticados por meio de redes descentralizadas — como blockchain ou sistemas de anonimização — a identificação do agente ativo se torna uma tarefa quase impossível. A ausência de um centro de controle, aliada ao uso de criptografia e anonimização, compromete a atribuição individual da conduta. Assim, o conceito clássico de autoria, que pressupõe domínio do fato, é insuficiente para lidar com crimes em que a ação é diluída entre diversos usuários ou executada de forma automatizada[177]

A análise do dolo também enfrenta desafios inéditos. Em crimes digitais, a intenção criminosa pode ser compartilhada entre programadores, operadores e até mesmo sistemas autônomos capazes de agir sem intervenção humana direta. A fronteira entre dolo e culpa se torna nebulosa quando o agente apenas desencadeia um processo tecnológico cujo resultado delitivo decorre de aprendizado de máquina ou automação. Essa ambiguidade questiona a própria essência da imputação penal clássica[178] .

A consumação dos crimes digitais, por sua vez, também desafia a dogmática penal. Em delitos de invasão, por exemplo, o momento exato em que o crime se consuma — se no acesso não autorizado, na extração de dados ou no uso indevido da informação — é objeto de intensos debates doutrinários. Essa indeterminação prejudica a definição de tentativa e consumação, exigindo novas categorias de tempo e espaço jurídico para os crimes informáticos[179] .

Outro aspecto crítico é o papel da automação na execução de delitos. Bots e algoritmos podem realizar ataques, disseminar desinformação ou executar transações fraudulentas sem participação humana direta, o que desafia o princípio da culpabilidade. Quando a conduta é mediada por um sistema automatizado, o agente humano perde o controle total do resultado, tornando a imputação penal mais complexa e exigindo uma revisão das teorias tradicionais de autoria mediata e coautoria[180].

A dificuldade de imputar responsabilidade em crimes tecnológicos está diretamente

[176] FRUMI, 2022, p. 147.
[177] MOTA, 2020, p. 115.
[178] ALVES et al., 2024, p. e4349.
[179] GOMES, 2024, p. 22.
[180]ARAÚJO, Victor Melo. Segurança Da Informação. Clube de Autores, 2015. p. 61

relacionada ao avanço das técnicas de invasão e à sofisticação das ferramentas digitais. Ataques como phishing, DDoS e ransomware são realizados por meio de estruturas distribuídas globalmente, nas quais o criminoso se esconde entre múltiplos endereços IP e servidores intermediários. Essa descentralização cria uma cadeia de atos e intenções que não se encaixa nos moldes da ação unitária prevista pelo Direito Penal clássico[181]

Os crimes de manipulação digital, como as *deepfakes*, ilustram de forma contundente a insuficiência da estrutura clássica de tipificação. A criação de conteúdo falso automatizado levanta dúvidas sobre quem deve ser considerado o autor — o programador, o operador do sistema ou o usuário que divulga o material. A ausência de clareza sobre o elemento subjetivo da ação impede uma resposta penal uniforme, expondo a necessidade de modernização legislativa e doutrinária[182].

Autores como Mitnick e Simon destacam que o componente humano ainda desempenha papel crucial, mesmo em sistemas automatizados. A engenharia social e a manipulação psicológica continuam sendo os vetores mais explorados por criminosos digitais, o que indica que, apesar da tecnologia, o dolo frequentemente permanece vinculado à intenção humana inicial. No entanto, a expansão da autonomia tecnológica exige uma redefinição dos limites da responsabilidade e da previsibilidade penal[183]

A insuficiência da estrutura clássica de tipificação demonstra que o Direito Penal precisa evoluir para abarcar condutas praticadas em ambientes digitais descentralizados e automatizados. A reformulação dos conceitos de autoria, dolo e consumação não deve enfraquecer as garantias constitucionais, mas sim adaptá-las a uma nova realidade tecnológica. A compatibilização entre avanço científico e segurança jurídica será o principal desafio para o legislador e para a doutrina penal nas próximas décadas[184]

O avanço vertiginoso das tecnologias digitais impõe ao Direito Penal um desafio de atualização permanente. Novas modalidades de crimes, como invasões automatizadas, fraudes eletrônicas e manipulação digital de informações, surgem em um ritmo que o legislador dificilmente consegue acompanhar. Essa defasagem entre inovação criminosa e produção normativa tem levado à ampliação interpretativa das normas penais existentes, o que, embora necessário para dar resposta aos delitos modernos, pode resultar em afronta ao princípio da legalidade e à segurança jurídica[185]

---

[181] FRAGA; VANGLLER, 2017, p. 234.
[182] BARBOSA; CEZAR; CARVALHO, 2024, p. 4.
[183] MITNICK; SIMON, 2003, p. 51.
[184] BOTELHO et al., 2023, p. 2723.
[185] HERNANDEZ; TOLEDO, 2021, p. 74.

A aplicação extensiva do Direito Penal a situações não previstas expressamente em lei revela o risco de se utilizar a analogia in malam partem, prática vedada pelo ordenamento jurídico brasileiro. A tentativa de enquadrar crimes digitais em tipos penais tradicionais, sem respaldo legislativo adequado, compromete a coerência dogmática e enfraquece as garantias individuais. O princípio da legalidade exige previsibilidade e precisão normativa, elementos que se perdem quando o intérprete se vê obrigado a adaptar a lei a realidades tecnológicas para as quais ela não foi concebida[186]

O fenômeno do estupro virtual, por exemplo, ilustra a necessidade urgente de atualização legislativa. Embora provoque danos morais e psicológicos equivalentes ao estupro físico, o crime é de difícil enquadramento pela ausência de contato corporal — elemento essencial na tipificação tradicional. Essa lacuna normativa exige que o legislador formule novas categorias penais, capazes de refletir a natureza imaterial e digital das ofensas, sem recorrer a expansões interpretativas que distorcem o texto legal[187]

As práticas de *cyberstalking* e de disseminação de *deepfakes* também evidenciam as limitações do Direito Penal clássico. A ausência de previsão legal específica para certas condutas obriga a jurisprudência a improvisar soluções hermenêuticas, ora tratando-as como injúria, ora como difamação ou falsificação. Essa elasticidade interpretativa, embora bem-intencionada, fere o núcleo garantista do Direito Penal, transformando-o em um campo de incertezas e subjetividades[188] .

A expansão interpretativa tem, ainda, um impacto direto sobre a função preventiva da norma penal. Quando o cidadão não consegue compreender com clareza quais condutas são puníveis, a eficácia pedagógica da lei é enfraquecida. A insegurança jurídica resultante desse processo mina a confiança social no sistema de justiça e reduz a legitimidade do poder punitivo estatal, que passa a atuar de forma imprevisível e potencialmente arbitrária[189] .

O advento das tecnologias descentralizadas e da inteligência artificial complexifica ainda mais esse cenário. Sistemas autônomos podem agir sem controle direto do ser humano, tornando incertas as noções de dolo, culpa e autoria. A ausência de critérios dogmáticos claros sobre a imputação penal nesses casos abre espaço para interpretações criativas, que frequentemente extrapolam os limites da legalidade e comprometem os princípios constitucionais do Estado Democrático de Direito[190] .

---

[186] GUERRA; CANDEIA, 2022, p. 3.
[187] GUERRA; CANDEIA, 2022, p. 5.
[188] MOTA, 2020, p. 119.
[189] COLAÇO, 2017, p. 10.
[190] ALVES et al., 2024, p. e4350.

A atualização dogmática do Direito Penal deve, portanto, ocorrer dentro de parâmetros estritamente constitucionais, sem sacrificar as garantias individuais em nome da eficiência punitiva. O enfrentamento da criminalidade tecnológica exige não apenas novas leis, mas também uma reflexão sobre a estrutura conceitual do próprio Direito Penal, de modo a incorporar as especificidades do ambiente digital sem violar o princípio da reserva legal[191]

Além da reforma legislativa, é indispensável uma evolução na formação dos operadores do direito. Juízes, promotores e advogados precisam dominar conceitos técnicos de segurança da informação, redes descentralizadas e criptografia, a fim de interpretar corretamente os elementos das condutas digitais. Sem esse conhecimento especializado, há o risco de que decisões judiciais baseadas em equívocos técnicos ampliem de forma indevida o alcance da norma penal[192] .

A atualização dogmática e legislativa deve buscar equilíbrio entre inovação e garantismo. A criação de novos tipos penais para condutas digitais é necessária, mas deve respeitar os limites impostos pela legalidade e pela taxatividade. A expansão interpretativa, quando desmedida, coloca em risco a previsibilidade normativa e transforma o Direito Penal em instrumento de exceção, contrariando sua função protetiva no Estado de Direito[193] .

4.4 Crimes digitais, metaverso e os desafios dogmáticos do Direito Penal

A emergência do metaverso — ambiente virtual imersivo e descentralizado, sustentado por tecnologias como blockchain e realidade aumentada — inaugura novos desafios para o Direito Penal. A principal problemática reside na imputação penal, ou seja, na identificação do agente e na delimitação da conduta típica em um espaço onde a interação é mediada por avatares e sistemas automatizados. A dissociação entre a identidade física e a representação digital do indivíduo fragiliza os mecanismos tradicionais de responsabilização penal, exigindo uma revisão dos conceitos de autoria e dolo[194] .

Nesse contexto, a determinação da autoria no metaverso torna-se complexa devido à natureza descentralizada das plataformas e à possibilidade de anonimato quase absoluto. O agente pode operar sob identidades falsas, utilizar redes privadas virtuais (VPNs) ou empregar inteligência artificial para executar condutas criminosas sem deixar rastros pessoais. Essa

[191] GOMES, 2024, p. 28.
[192] HERNANDEZ; TOLEDO, 2021, p. 78.
[193] BARBOSA; CEZAR; CARVALHO, 2024, p. 4.
[194] SILVA et al., 2023, p. 75.

fragmentação da identidade compromete a aplicação direta do princípio da pessoalidade da pena, desafiando os fundamentos do sistema penal clássico[195] .

Além disso, a delimitação da conduta típica enfrenta entraves inéditos. No ambiente físico, a ação criminosa é delimitada por tempo, espaço e intenção; no metaverso, essas fronteiras tornam-se difusas. Um ato de difamação, invasão de propriedade virtual ou assédio cometido por um avatar pode ocorrer simultaneamente em múltiplos servidores e países, tornando a tipificação dependente de interpretações jurídicas transnacionais e de cooperação internacional[196].

O dolo digital surge como nova categoria teórica necessária para compreender a intencionalidade das condutas no metaverso. Diferentemente do dolo tradicional, ele se manifesta por meio de comandos programados, scripts ou interações automatizadas que expressam a vontade criminosa de forma mediada pela tecnologia. Essa reconfiguração do dolo desafia a teoria clássica da ação e exige um redimensionamento do conceito de vontade dirigida a um resultado[197] .

Outro aspecto crítico diz respeito à territorialidade do delito. O metaverso não reconhece fronteiras geográficas: um crime pode ser praticado em ambiente hospedado em servidores estrangeiros, vitimando pessoas de diferentes nacionalidades. Essa descentralização desafia o artigo 6º do Código Penal brasileiro, que define a aplicação da lei penal no espaço, e impõe a necessidade de tratados internacionais específicos para regular a jurisdição e a cooperação em casos de delitos imersivos[198] .

Os crimes de natureza sexual e patrimonial ganham novas dimensões nesse ambiente. Práticas como o estupro virtual e o furto de ativos digitais exigem uma análise minuciosa sobre a materialidade da conduta e a extensão do dano. No caso do estupro virtual, a ausência de contato físico não elimina o constrangimento psicológico ou a violação da dignidade da vítima, o que reforça a necessidade de repensar os critérios de tipificação penal sob a ótica dos direitos fundamentais[199] .

A imputação penal no metaverso também demanda uma reflexão sobre a responsabilidade de intermediários tecnológicos, como desenvolvedores e provedores de plataformas. A linha tênue entre culpa e dolo eventual se torna ainda mais frágil quando tais

[195] TAVARES, 2012, p. 166.
[196] BARROSO, 2018, p. 412.
[197] BOTELHO et al., 2023, p. 2718.
[198] SOUZA; CERVINSKI, 2021, p. 7.
[199] DORIGON, 2024, p. 4.

agentes têm conhecimento prévio da vulnerabilidade de seus sistemas e nada fazem para evitar que crimes ocorram. A responsabilização por omissão digital, portanto, é um tema que ganha relevância diante do papel ativo das empresas na manutenção desses ecossistemas virtuais[200] .

Há ainda o risco de que a expansão punitiva, impulsionada pela insegurança jurídica, leve à violação do princípio da legalidade. A ausência de tipos penais específicos para o metaverso não autoriza interpretações analógicas ou extensivas em prejuízo do acusado. O desafio legislativo, portanto, consiste em equilibrar inovação normativa e segurança jurídica, criando dispositivos precisos que abranjam as novas formas de interação digital sem romper com as garantias constitucionais[201] .

O estudo da imputação penal no metaverso evidencia que o Direito Penal tradicional não pode ser simplesmente transplantado para o ambiente virtual. É preciso construir uma nova dogmática que considere a imaterialidade das ações, a multiplicidade de jurisdições e o protagonismo das tecnologias autônomas. Somente por meio de uma abordagem interdisciplinar — combinando Direito, tecnologia e filosofia jurídica — será possível preservar os princípios da legalidade, culpabilidade e proporcionalidade diante das incertezas do universo digital imersivo[202] .

A construção de uma dogmática penal compatível com a realidade aumentada, o metaverso e as interações simuladas exige um reposicionamento metodológico do Direito Penal: não se trata apenas de criar novos tipos penais tecnológicos, mas de assegurar que essa atualização ocorra sem ruptura com os princípios constitucionais, especialmente a legalidade, a taxatividade e a anterioridade. A legalidade continua a ser a âncora que impede o arbítrio estatal, mas ela é testada em um ambiente no qual a fronteira entre conduta física e conduta digital se dilui. O que antes era concebido como ato material, tangível e espacialmente localizado passa, nesses novos ambientes, a ser ato informacional, performado por avatares, algoritmos e interfaces aumentadas, o que obriga a doutrina penal a redefinir categorias como ação, autoria, resultado e ofensa ao bem jurídico[203] .

Essa necessidade de reconstrução dogmática não pode ser confundida com flexibilização das garantias. Ao contrário, o ambiente virtual torna ainda mais urgente a preservação rigorosa da legalidade, sob pena de permitir que juízes e órgãos persecutórios ampliem o alcance de tipos penais a condutas que não foram previstas pelo legislador. Em

[200] SILVA et al., 2023, p. 81.
[201] BARROSO, 2018, p. 420.
[202] BOTELHO et al., 2023, p. 2722.
[203] COSTA, 2021, p. 12.

crimes praticados em realidades aumentadas — como assédio direcionado por meio de hologramas, perseguição contínua via avatar, ou exposição íntima não consentida em ambientes simulados — a tentação de punir com base em analogias é grande, mas isso violaria frontalmente a taxatividade e desorganizaria o sistema penal, que deixaria de ser regido por normas gerais e abstratas para se converter em um instrumento casuístico e reativo[204] .

A realidade aumentada adiciona outra camada de complexidade: ela funde o mundo físico e o digital, criando situações em que o dano psicológico, reputacional ou patrimonial ocorre no plano concreto, embora a ação causal tenha ocorrido no plano virtual. Essa fusão desafia a distinção clássica entre ato e efeito, tão central para a determinação da consumação do crime. Em casos como deepfakes projetadas publicamente, simulações de nudez da vítima em ambientes imersivos ou perseguição algorítmica e geolocalizada, a agressão à dignidade extrapola a "virtualidade" e afeta bens jurídicos reais, o que exige uma releitura do conceito de lesão relevante para o Direito Penal sem violar o devido processo legal[205] .

Essa reconfiguração também tem dimensão internacional. A circulação de condutas ilícitas em ambientes simulados não respeita fronteiras estatais e coloca em tensão princípios clássicos como soberania e territorialidade. A dificuldade em definir onde o crime foi praticado — se no servidor, no dispositivo do agente ou no local em que a vítima experimentou o dano — desafia diretamente a aplicação espacial da lei penal. Isso impõe a necessidade de uma coordenação normativa transnacional que preserve a legalidade, no sentido de evitar conflitos de jurisdição ou sobreposição punitiva arbitrária entre Estados que disputem competência sobre um mesmo fato delitivo virtual[206] .

A imputação penal nas interações simuladas também exige um olhar cuidadoso para o elemento subjetivo. Em muitos casos, o agente utiliza ferramentas técnicas para potencializar sua conduta lesiva: bots de assédio, scripts automatizados de coleta de dados, filtros de voz que ocultam identidade, ou ainda manipulação psicológica em tempo real sobre a vítima em ambiente imersivo. A engenharia social, já descrita como uma arma criminosa baseada em manipulação comportamental e não apenas em tecnologia, mostra que a intenção criminosa pode se realizar por meios sutis e persuasivos que escapam do padrão físico de ameaça ou coação. Isso reforça que a vontade criminosa pode se manifestar sem contato físico direto, mas ainda assim com clara finalidade lesiva, o que a dogmática penal não pode ignorar[207] .

---

[204] WERMUTH; CALLEGARI, 2021, p. 117.
[205] MERLONE, 2025, p. 14.
[206] PORTELA, 2025, p. 233.
[207] MITNICK; SIMON, 2003, p. 45.

Do ponto de vista da política criminal, a virtualidade amplia a escala e o impacto potencial das condutas ilícitas. Um assédio dirigido a uma única vítima em ambiente presencial torna-se, no metaverso, um ato replicável contra dezenas ou centenas de usuários em poucos segundos, por meio de scripts automatizados e replicação de conteúdo. Essa dimensão de massa do dano social pressiona o legislador a reagir de modo mais severo e abrangente, mas tal reação precisa ser controlada pelos limites constitucionais da proporcionalidade e da intervenção mínima, sob pena de transformar o Direito Penal em instrumento de controle generalizado sobre discursos e interações digitais[208] .

A prevenção e a governança dos ambientes imersivos surgem, então, como parte da resposta necessária. Não basta apenas tipificar novas condutas: é indispensável que plataformas virtuais, empresas de tecnologia e órgãos públicos compartilhem responsabilidades na prevenção de violações e na identificação de autores. A responsabilização de intermediários tecnológicos, entretanto, não pode ocorrer de forma ilimitada, sob pena de instaurar uma censura privada e um policiamento algorítmico sem controle judicial. A compatibilidade entre legalidade e virtualidade depende de encontrar um ponto de equilíbrio entre deveres de colaboração técnica e limites constitucionais à responsabilização automática de provedores[209] .

Outro desafio central é garantir que a proteção penal no ambiente virtual não seja capturada por narrativas de pânico moral. O medo social produzido por crimes cibernéticos de alta repercussão pode gerar demandas por legislações emergenciais e punitivistas, que tendem a abrir tipos penais vagos para abarcar qualquer conduta “suspeita” em realidade aumentada. Esse tipo de expansão casuística, ainda que bem-intencionada, ameaça diretamente o princípio da legalidade e fragiliza a segurança jurídica. A dogmática penal deve atuar como barreira racional, lembrando que a criação de crimes deve ser precisa, necessária e proporcional, e não fruto de reação emocional[210] .

A compatibilidade entre legalidade e virtualidade só será viável se o Direito Penal reconhecer o caráter estrutural da virtualização das relações humanas. Não se trata de fenômeno transitório, mas de uma nova dimensão da vida social. Isso exige uma metodologia penal que integre tecnologia, proteção de bens jurídicos informacionais e garantias constitucionais. A legalidade, nesse cenário, não é um obstáculo ao enfrentamento dos crimes digitais: ela é precisamente o instrumento que assegura que a repressão não se converta em vigilância

[208] BOTELHO et al., 2023, p. 2720.
[209] COSTA, 2021, p. 28).
[210] SOUZA; CERVINSKI, 2021, p. 8.

desmedida ou controle comportamental. Em outras palavras, preservar o princípio da legalidade em ambientes simulados é o que mantém viva a distinção entre um Direito Penal constitucional e um Direito Penal de exceção[211] .

5 Jurisdição penal no ciberespaço

A expansão das fronteiras digitais redefiniu o conceito de espaço jurídico, impondo novos desafios à aplicação da jurisdição penal. No ciberespaço, as condutas criminosas ultrapassam barreiras territoriais em questão de segundos, desafiando os princípios tradicionais que regem a aplicação da lei penal no tempo e no espaço. Essa nova realidade exige que o Direito Penal abandone sua concepção puramente territorial e desenvolva instrumentos capazes de lidar com a natureza descentralizada e transnacional da internet. Assim, o estudo da jurisdição penal digital torna-se indispensável para compreender como os Estados podem exercer seu poder punitivo de forma legítima e coordenada, sem violar a soberania alheia ou gerar conflitos de competência.

A análise da jurisdição penal no ciberespaço demanda uma abordagem integrada entre o Direito Interno e o Direito Internacional. O ambiente digital abriga práticas criminosas que envolvem múltiplos agentes, países e servidores, o que torna essencial o fortalecimento de mecanismos de cooperação jurídica, como tratados multilaterais e acordos de assistência mútua. Ao mesmo tempo, surge a necessidade de repensar a aplicação dos princípios da territorialidade, extraterritorialidade e ubiquidade diante de fenômenos emergentes, como o metaverso e as criptotransações ilícitas. O desafio contemporâneo consiste em equilibrar eficiência investigativa e respeito às garantias fundamentais, construindo uma jurisdição penal que seja,

[211] WERMUTH; CALLEGARI, 2021, p. 123.

ao mesmo tempo, tecnológica, colaborativa e constitucionalmente legítima.

5.1 Princípios de aplicação da lei penal no espaço digital

A expansão das interações humanas para o ambiente digital trouxe à tona novos desafios à aplicação da lei penal, sobretudo quanto à delimitação espacial dos delitos virtuais. A internet rompe as fronteiras físicas, criando uma multiplicidade de jurisdições possíveis e exigindo uma revisão dos princípios tradicionais da territorialidade e da ubiquidade. A definição do locus delicti torna-se, portanto, complexa, uma vez que a conduta e o resultado podem ocorrer em países distintos, fragmentando a persecução penal e dificultando a atribuição de competência às autoridades nacionais[212]

O princípio da territorialidade, base do direito penal clássico, estabelece que a lei penal de um país aplica-se aos fatos ocorridos dentro de seu território. No entanto, quando se trata de crimes cibernéticos, a localização do agente, do servidor ou da vítima pode não coincidir. Assim, o princípio da ubiquidade, que admite o local da ação ou do resultado como determinante da competência, passa a ser aplicado com maior flexibilidade, buscando adaptar-se à fluidez dos ambientes digitais[213].

Essa necessidade de adaptação também é reconhecida no contexto internacional, em que a cooperação jurídica se torna instrumento essencial para a eficácia da jurisdição penal. A soberania estatal, outrora delimitada por fronteiras físicas, passa a ser tensionada por redes interconectadas globalmente. Surge, assim, um novo paradigma de aplicação do direito penal, em que a territorialidade precisa coexistir com a natureza transnacional dos dados e das condutas[214] .

A descentralização das infraestruturas tecnológicas, como servidores em nuvem e redes distribuídas, acentua ainda mais a dificuldade de identificar o local exato da prática do crime. Essa fragmentação técnica desafia os critérios tradicionais de competência territorial, exigindo novos modelos interpretativos que contemplem a ubiquidade digital como princípio orientador da persecução penal[215].

Ao mesmo tempo, a aplicação do direito penal deve respeitar os limites constitucionais

---

[212] BRASIL, 2014, p. 1.
[213] COSTA, Fernando José da. Locus delicti nos crimes informáticos. 2011. Tese de Doutorado. Universidade de São Paulo. p. 78.
[214] PORTELA, 2025, p. 214.
[215] LÓSSIO, Claudio Joel Brito. O Direito e o ciberespaço. São Paulo: Editora JusPodivm, 2022. p. 53.

da legalidade e da segurança jurídica, evitando que a expansão interpretativa resulte em violações de garantias fundamentais. O ambiente digital, embora novo, não autoriza o abandono das bases dogmáticas do direito penal, devendo-se conciliar inovação tecnológica com previsibilidade normativa[216] .

Outro aspecto relevante é a responsabilidade compartilhada entre os provedores de serviços e as autoridades nacionais. A atuação dessas empresas, muitas vezes sediadas no exterior, interfere diretamente na eficácia da jurisdição penal, sobretudo no fornecimento de dados e na preservação de evidências digitais. Essa relação jurídica é permeada por conflitos de competência e pela necessidade de harmonizar normas de privacidade e de cooperação[217] .

A legislação brasileira, especialmente o Marco Civil da Internet, buscou estabelecer critérios objetivos para o tratamento de dados e a atuação jurisdicional sobre provedores. Ao determinar que a lei brasileira se aplica a serviços ofertados no território nacional, independentemente do local do servidor, o texto legal reforça a soberania digital do Estado e amplia o alcance da lei penal sobre condutas praticadas em rede[218] .

Entretanto, ainda há lacunas na forma como o direito penal lida com os efeitos extraterritoriais dos crimes digitais. Casos de fraudes financeiras, vazamento de dados e disseminação de material ilícito demonstram que a jurisdição, muitas vezes, depende mais da capacidade técnica de investigação do que dos limites territoriais. Assim, propõe-se uma interpretação funcional dos princípios penais, voltada para a efetividade da tutela jurídica[219] .

O avanço tecnológico impõe a necessidade de um modelo de jurisdição adaptável, no qual o Estado reconheça a complexidade do ciberespaço sem renunciar à proteção dos bens jurídicos fundamentais. O equilíbrio entre territorialidade e globalidade jurídica deve nortear a aplicação da lei penal digital, garantindo que a justiça acompanhe a velocidade da inovação sem comprometer os pilares do Estado de Direito[220] .

A ampliação do espaço digital também trouxe consigo a multiplicidade de agentes, plataformas e jurisdições envolvidas em um mesmo ato ilícito. Crimes como fraudes eletrônicas, invasões de sistemas e disseminação de desinformação frequentemente envolvem diferentes atores localizados em diversos países, tornando a investigação dependente da cooperação internacional. Nesse sentido, a articulação entre autoridades nacionais e

[216] SOUZA; CERVINSKI, 2021, p. 5.
[217] COLAÇO, 2017, p. 10.
[218] BRASIL, 2014, p. 2.
[219] COSTA, 2011, p. 81.
[220] PORTELA, 2025, p. 216.

estrangeiras torna-se indispensável, uma vez que a eficácia da jurisdição penal digital depende da capacidade de se obter provas e identificar autores em redes globalizadas[221] .

Ademais, o desafio da territorialidade digital não se restringe à questão técnica, mas também envolve dilemas éticos e políticos. A aplicação extraterritorial da lei penal brasileira, por exemplo, deve respeitar a soberania de outros Estados e os tratados internacionais vigentes. A ausência de um consenso global sobre os limites do exercício jurisdicional no ciberespaço pode gerar conflitos diplomáticos e decisões contraditórias, enfraquecendo a efetividade da repressão penal. Torna-se, portanto, imprescindível o desenvolvimento de diretrizes multilaterais que uniformizem critérios de jurisdição e assegurem a cooperação recíproca entre os países[222] .

Outro ponto crucial é a questão probatória no contexto digital. A localização dos servidores e a volatilidade dos dados armazenados em nuvem dificultam a aplicação dos princípios da legalidade e da cadeia de custódia. As provas digitais, por serem facilmente alteráveis e reproduzíveis, exigem protocolos específicos de coleta e preservação, sob pena de nulidade processual. Dessa forma, o fortalecimento das normas técnicas de segurança da informação torna-se essencial para garantir a validade das evidências e a integridade das investigações[223] .

A doutrina contemporânea tem apontado ainda para a necessidade de uma interpretação dinâmica da territorialidade, compatível com a ubiquidade das ações cibernéticas. Isso significa compreender que o crime digital não ocorre em um ponto fixo, mas em uma rede de conexões simultâneas que ultrapassam fronteiras físicas e temporais. Essa nova abordagem não enfraquece o poder estatal, mas o redefine, permitindo que a jurisdição penal atue de forma mais eficaz e contextualizada diante da fluidez tecnológica[224] .

A consolidação de uma jurisdição penal eficiente no espaço digital depende da conjugação entre infraestrutura tecnológica e capacidade institucional. O Estado deve investir em perícias digitais, formação de especialistas e criação de unidades especializadas em crimes cibernéticos, capazes de compreender tanto os aspectos técnicos quanto jurídicos das infrações. Somente com uma estrutura integrada e tecnicamente preparada será possível aplicar de maneira justa e eficaz os princípios da lei penal no ciberespaço[225] .

---

[221] BRASIL, 2014, p. 3.
[222] PORTELA, 2025, p. 219.
[223] COSTA, 2011, p. 84.
[224] LÓSSIO, 2022, p. 61.
[225] SOUZA; CERVINSKI, 2021, p. 7.

5.2 Territorialidade e extraterritorialidade em crimes cibernéticos

A globalização digital desafia as fronteiras tradicionais do Direito Penal, especialmente quando se trata da aplicação da lei a condutas que ocorrem fora do território nacional, mas produzem efeitos dentro dele. No contexto dos crimes cibernéticos, a noção de territorialidade adquire um caráter fluido, pois as ações criminosas podem ser iniciadas em um país e causar danos em outro, exigindo interpretações jurídicas que conciliem soberania e cooperação. A legislação brasileira, ao estabelecer hipóteses de aplicação extraterritorial da lei penal, busca preservar a tutela de bens jurídicos nacionais sem desconsiderar a dimensão global das condutas digitais[226]
.

A extraterritorialidade condicionada surge como instrumento essencial na persecução penal de crimes transnacionais, especialmente quando os atos violam interesses do Estado ou atingem cidadãos brasileiros. Em casos como fraudes eletrônicas, disseminação de dados pessoais e invasões de sistemas, a persecução penal depende da existência de duplo reconhecimento do crime — no país de origem e no de destino da conduta[227]. Essa exigência visa resguardar o princípio da legalidade e evitar abusos na expansão da jurisdição estatal.

A análise da territorialidade em ambiente digital revela que o conceito de "lugar do crime" precisa ser reinterpretado. Nas infrações informáticas, a ação pode ocorrer em múltiplos locais simultaneamente — o que inviabiliza uma definição única de locus delicti. A doutrina brasileira propõe, portanto, o uso da teoria da ubiquidade, que considera tanto o local da execução quanto o da produção do resultado como competentes para a aplicação da lei penal[228].

Outro desafio relevante está na produção e validação das provas em processos transnacionais. A obtenção de dados digitais localizados em servidores estrangeiros demanda observância à cadeia de custódia e aos tratados de cooperação internacional. O Código de Processo Penal, ao disciplinar a preservação e integridade das evidências eletrônicas, reforça a necessidade de rastreabilidade e autenticidade como requisitos para a validade da persecução penal[229]

Além da dimensão penal, há implicações civis e administrativas decorrentes da territorialidade digital. As plataformas de tecnologia, muitas vezes sediadas fora do Brasil,

---

[226] BRASIL, 2023, p. 2.
[227] PRESTES, Felipe Pinheiro; ANACLETO, Elvis Preis. JURISDIÇÃO CRIMINAL E DELITOS INFORMÁTICOS: REFLEXOS NA JURISDIÇÃO BRASILEIRA DA CONVENÇÃO DE BUDAPESTE. Anais do Seminário Internacional em Direitos Humanos e Sociedade, v. 6, 2024. p. 8.
[228] COSTA, 2011, p. 102.
[229] BRASIL, 2023, p. 5.

tornam-se sujeitos indiretos da jurisdição nacional ao fornecerem serviços acessíveis no território brasileiro. O Marco Civil da Internet determina que empresas que ofertam serviços ao público brasileiro estão sujeitas às leis locais, mesmo que operem de forma remota, reforçando a soberania digital do Estado[230] .

Contudo, a aplicação da lei brasileira a empresas estrangeiras gera controvérsias sobre limites de jurisdição e alcance da responsabilidade. Doutrinadores defendem que, embora o Brasil tenha autonomia para proteger seus cidadãos, a efetividade dessa proteção depende da colaboração voluntária ou compulsória das empresas provedoras. A jurisprudência internacional vem consolidando entendimentos que equilibram privacidade, segurança e dever de cooperação, conforme apontado em estudos sobre responsabilidade de provedores[231] .

Os crimes cibernéticos de natureza transnacional também levantam discussões sobre soberania e segurança informacional. A circulação de dados sensíveis entre países exige políticas de proteção integradas e compatíveis com o princípio da reciprocidade. Assim, a aplicação extraterritorial da lei penal deve ser interpretada de forma harmônica com o Direito Internacional Público, preservando a cooperação sem violar a autonomia dos Estados[232] .

Outro ponto de atenção refere-se às barreiras técnicas que dificultam a identificação dos agentes criminosos em redes distribuídas e anônimas. A engenharia social e o uso de tecnologias de criptografia permitem a execução de ataques sem fronteiras visíveis, o que fragiliza a eficácia da jurisdição tradicional. A superação desses desafios depende tanto da modernização legal quanto do aprimoramento das políticas de segurança da informação[233] .

A territorialidade e a extraterritorialidade devem ser vistas não como conceitos excludentes, mas complementares na era digital. Enquanto a primeira assegura a soberania nacional sobre os fatos ocorridos em seu domínio, a segunda possibilita o alcance penal sobre condutas que, embora transnacionais, produzem efeitos concretos no país. O equilíbrio entre essas dimensões é essencial para garantir a efetividade da justiça e a proteção dos direitos fundamentais no ciberespaço[234].

5.3 Jurisdição penal e os espaços regulados da internet

[230] FRUMI, 2022, p. 148.
[231] COLAÇO, 2017, p. 9.
[232] PORTELA, 2025, p. 187.
[233] ARAÚJO, 2015, p. 44.
[234]LEONARDI, Marcel. Responsabilidade civil dos provedores de serviços de internet. Editora Juarez de Oliveira, 2005. p. 112

A internet consolidou-se como um ambiente multifacetado, composto por plataformas privadas que estabelecem suas próprias normas internas e mecanismos de moderação de conteúdo. Esses espaços regulados coexistem com a jurisdição estatal, criando um cenário de sobreposição entre normas jurídicas e políticas corporativas. As grandes empresas de tecnologia, ao controlarem fluxos de informação e dados, acabam desempenhando papel quase normativo, impondo regras de conduta que muitas vezes transcendem as fronteiras nacionais. Esse fenômeno desafia o alcance da jurisdição penal tradicional e exige uma reflexão sobre o equilíbrio entre regulação pública e governança privada[235] .

Os provedores estrangeiros, especialmente aqueles sediados em países com legislações protetivas de privacidade, frequentemente resistem a solicitações judiciais de autoridades brasileiras. Essa resistência se apoia na diferença de regimes jurídicos e na ausência de tratados específicos para o compartilhamento rápido de informações. A jurisdição nacional, diante disso, enfrenta obstáculos para impor suas decisões a empresas que, embora operem no Brasil, não mantêm representação física ou servidores localizados no território nacional[236] .

A ascensão das plataformas em nuvem e dos serviços descentralizados de armazenamento ampliou a complexidade das investigações criminais. A dispersão geográfica dos dados e a criptografia dificultam a execução de ordens judiciais, impondo a necessidade de novas estratégias de cooperação técnica e jurídica. Além disso, as normas de proteção de dados pessoais, como a LGPD, impõem limites ao compartilhamento de informações, demandando uma atuação equilibrada entre privacidade e repressão penal[237] .

O conceito de "espaço regulado" da internet vai além da dimensão técnica — abrange também a lógica contratual dos termos de uso e das políticas de compliance internas. Esses instrumentos funcionam como códigos normativos privados que, embora não tenham força de lei, impactam diretamente a aplicação da legislação penal, especialmente em casos de exclusão de conteúdos ilícitos ou fornecimento de provas. As cláusulas de uso e de cooperação, muitas vezes, são redigidas de modo a restringir a atuação de autoridades públicas fora da jurisdição da empresa[238].

A interação entre as jurisdições nacionais e as plataformas digitais cria um campo híbrido, no qual as empresas assumem funções regulatórias complementares às do Estado. Essa

[235] LEONARDI, 2005, p. 115.
[236] BRASIL, 2012, p. 2.
[237] ARAÚJO, 2015, p. 91.
[238]ALEXANDRIA, JCS de. Gestão de Segurança da Informação–uma proposta para potencializar a efetividade da Segurança da Informação em ambiente de pesquisa científica. Instituto de Pesquisas Energéticas e Nucleares, Universidade de São Paulo, São Paulo, 2009. p. 63

coexistência, porém, gera tensões sobre legitimidade e controle. Enquanto os provedores se justificam pela necessidade de padronização global, os Estados reivindicam sua competência soberana para proteger os cidadãos e assegurar a efetividade das leis internas[239].

No âmbito penal, a ausência de mecanismos ágeis de cooperação entre o poder público e os provedores afeta diretamente a produção de provas digitais. Em muitos casos, o tempo de resposta para o fornecimento de registros ou a remoção de conteúdos ilícitos compromete a persecução penal. Essa lentidão evidencia a importância de políticas de compliance bem estruturadas, que possam funcionar como instrumentos de autorregulação compatíveis com as exigências legais e processuais nacionais[240] .

Por outro lado, é inegável que os provedores desempenham um papel essencial na proteção dos direitos fundamentais no ambiente virtual. A implementação de medidas de segurança da informação e de detecção automática de comportamentos suspeitos contribui para prevenir a prática de crimes cibernéticos. Contudo, essa colaboração deve ocorrer dentro de limites legais claros, evitando que as empresas assumam funções investigativas que competem exclusivamente ao Estado[241] .

A literatura jurídica recente aponta para a necessidade de se reconhecer a internet como um espaço de múltiplas jurisdições, em que o diálogo entre direito público e governança privada é inevitável. As plataformas, ao definirem suas próprias regras de uso e sanções internas, acabam criando um "microssistema jurídico digital" que interage com o ordenamento estatal. A conciliação entre esses sistemas é essencial para garantir que as normas penais mantenham eficácia, sem suprimir a liberdade e a inovação que caracterizam o ambiente virtual[242].

Portanto, a jurisdição penal nos espaços regulados da internet deve ser entendida como um exercício compartilhado de autoridade. Cabe ao Estado reafirmar sua competência para coibir práticas ilícitas e assegurar a ordem jurídica, ao mesmo tempo em que reconhece o papel das empresas de tecnologia como parceiras estratégicas na prevenção e investigação de delitos. Somente por meio dessa integração será possível consolidar um modelo de governança digital que harmonize segurança, legalidade e respeito aos direitos fundamentais[243] .

5.4 Direito Penal, transnacionalidade e ciberespaço

[239] BERLANDA, Rodrigo Grando. Guia de segurança da informação para a conectividade de dispositivos IoT. 2021. p. 27
[240] LEONARDI, 2005, p. 102.
[241] ARAÚJO, 2015, p. 98.
[242]GOMES, Inês. Crimes contra a humanidade e ciberespaço. De Legibus-Revista de Direito da Universidade Lusófona Lisboa, n. 5e6, p. 65-100, 2023. p. 75.
[243] BERLANDA, 2021, p. 33).

A transnacionalidade é uma das marcas mais evidentes dos crimes praticados no ciberespaço. Diferentemente das infrações convencionais, os delitos digitais frequentemente ultrapassam fronteiras, envolvendo agentes, vítimas e infraestruturas distribuídas em múltiplos países. Esse fenômeno exige que o Direito Penal adote uma perspectiva internacionalizada, capaz de harmonizar normas e procedimentos para garantir a efetividade da persecução criminal. A ausência de uniformidade legislativa, entretanto, ainda representa um dos maiores desafios para a responsabilização dos agentes no ambiente digital[244].

A identificação e punição de condutas criminosas em redes globais dependem diretamente da cooperação entre Estados e instituições internacionais. Sem essa articulação, torna-se inviável o rastreamento de crimes como invasões de sistemas, fraudes eletrônicas e ataques de ransomware. A legislação nacional, como a Lei nº 12.737/2012, que tipifica os delitos informáticos, constitui um avanço importante, mas sua aplicação isolada é insuficiente diante da natureza transfronteiriça das condutas digitais[245] .

Os crimes cibernéticos desafiam os conceitos tradicionais de territorialidade e soberania, pois os efeitos de uma ação criminosa podem manifestar-se em países distintos daquele onde o agente atua. Nesse contexto, o Direito Penal deve dialogar com o Direito Internacional Público para definir mecanismos de jurisdição compartilhada e assistência mútua entre os Estados. Essa integração é essencial para equilibrar a proteção dos direitos fundamentais e a eficácia da repressão penal[246] .

Um dos maiores entraves à persecução penal transnacional é a ausência de tratados multilaterais que contemplem as particularidades da cibernética. Em muitos casos, as diferenças entre os ordenamentos dificultam a extradição de criminosos e o reconhecimento de provas digitais. A falta de padronização de procedimentos de coleta e preservação de evidências digitais compromete a validade jurídica das informações obtidas em investigações conjuntas[247]

A complexidade técnica dos crimes digitais também exige novas formas de colaboração entre autoridades públicas e o setor privado. As empresas de tecnologia, ao deterem o controle de servidores e sistemas de armazenamento de dados, desempenham papel central na detecção e notificação de incidentes. A engenharia social, por exemplo, revela como o comportamento

---

[244] SILVA, Amanda Scalisse. JURISDIÇÃO PENAL NA ERA DIGITAL: TERRITORIALIDADE E DELIMITAÇÃO JURISDICIONAL NO CIBERESPAÇO. In: Congresso Internacional de Direitos Humanos de Coimbra. 2024. p. 17.
[245] BRASIL, 2012.
[246] BARROSO, 2018, p. 243.
[247] GOMES, 2023, p. 71.

humano pode ser manipulado de modo transnacional, exigindo respostas conjuntas entre Estados e corporações[248] .

O ciberespaço, enquanto território imaterial, redefine a noção de jurisdição penal. As fronteiras deixam de ser barreiras geográficas e passam a depender de conexões tecnológicas. Essa transformação impõe a necessidade de repensar os princípios dogmáticos do Direito Penal, adaptando-os à realidade de crimes descentralizados e de autoria coletiva. Tavares destaca que a expansão digital obriga o Estado a reinterpretar seus limites de soberania e competência[249] .

Além da cooperação técnica, é indispensável fortalecer a cooperação jurídica internacional por meio de acordos bilaterais e mecanismos de troca rápida de informações. O modelo de assistência jurídica mútua (MLATs) é um instrumento valioso, mas ainda insuficiente diante da velocidade com que os crimes digitais se propagam. A construção de redes de confiança e o uso de protocolos seguros entre autoridades constituem um caminho promissor para superar barreiras burocráticas[250] .

A atuação penal no ciberespaço também demanda a observância de princípios constitucionais, como o devido processo legal, a ampla defesa e a legalidade. O combate a crimes transnacionais não pode justificar a relativização de garantias fundamentais. Assim, a transnacionalidade penal deve ser exercida sob parâmetros de legitimidade democrática e respeito aos direitos humanos, evitando excessos punitivistas em nome da segurança digital[251]

O Direito Penal contemporâneo precisa consolidar uma estrutura jurídica transnacional que seja, ao mesmo tempo, eficaz e garantista. O enfrentamento dos crimes cibernéticos só será possível mediante o alinhamento entre os ordenamentos jurídicos e a criação de canais de cooperação efetivos. O futuro da jurisdição penal no ciberespaço depende da capacidade dos Estados de agir em conjunto, preservando a justiça e a soberania em um ambiente que, por natureza, não conhece fronteiras[252] .

5.5 Crimes cibernéticos transnacionais e a cooperação jurídica

A criminalidade cibernética transnacional evidencia a interdependência entre os sistemas jurídicos e a necessidade de cooperação entre os Estados para garantir a efetividade

[248] COSTA; CRUZ, 2016, p. 4.
[249] TAVARES, 2012, p. 173.
[250] SILVA, 2024, p. 22.
[251] BARROSO, 2018, p. 247.
[252] GOMES, 2023, p. 89.

da persecução penal. A fluidez das fronteiras digitais permite que criminosos utilizem servidores e redes localizadas em diversos países, dificultando a aplicação da lei penal nacional. A resposta a esses desafios passa pela consolidação de mecanismos de assistência jurídica mútua, voltados à troca de informações e à coleta de provas digitais de forma célere e legítima[253]

A cooperação internacional é o eixo central da efetividade no combate aos crimes cibernéticos. Sem ela, o Estado nacional torna-se limitado na obtenção de dados de tráfego, registros de usuários e demais evidências armazenadas no exterior. A legislação brasileira, ao reconhecer a importância dessa integração, busca aprimorar os canais de comunicação com órgãos internacionais e plataformas tecnológicas, sem, contudo, abdicar de sua soberania jurisdicional[254]

No plano dogmático, a atuação penal além das fronteiras exige uma releitura dos princípios de territorialidade e soberania. A jurisdição, tradicionalmente vinculada ao território, precisa se adaptar à natureza global das infrações cibernéticas. A doutrina contemporânea propõe que o critério de aderência da jurisdição ao território seja relativizado, permitindo que o Estado atue quando os efeitos do crime se projetam em seu espaço jurídico[255].

As formas de assistência mútua internacional variam entre pedidos formais de cooperação, acordos multilaterais e tratados específicos. No contexto digital, destaca-se o uso de canais diretos entre autoridades policiais e plataformas privadas, os chamados *cross-border data requests*. Tais instrumentos reduzem a burocracia e ampliam a agilidade na obtenção de informações essenciais para investigações de fraudes, invasões de sistemas e disseminação de conteúdos ilícitos[256].

A coleta de provas digitais no exterior impõe novos desafios processuais. A falta de padronização nos procedimentos de autenticação e preservação de evidências compromete sua validade jurídica em tribunais nacionais. Por essa razão, o aprimoramento dos protocolos de cadeia de custódia e de intercâmbio seguro entre Estados é uma prioridade na agenda global da justiça criminal[257]

As novas tecnologias, ao mesmo tempo que ampliam o alcance das investigações, criam dilemas éticos e jurídicos relacionados à proteção de dados e à privacidade. A atuação

[253] SILVA, 2024, p. 15.
[254] BRASIL, 2012.
[255] SQUADRI, Ana Carolina. O princípio da aderência da jurisdição ao território na era digital. In: Revista de Processo. 2022. p. 473-483. p. 478.
[256] TEIXEIRA, André Álisson Leal. Jurisdição e internet: uma releitura da aplicação da lei processual penal no espaço à luz da escala mundial da internet. 2024. Tese de Doutorado. Universidade de São Paulo. p. 93.
[257] HERNANDEZ; DE TOLEDO, 2021, p. 79.

cooperativa entre autoridades precisa respeitar os limites constitucionais e o devido processo legal. O pragmatismo processual contemporâneo, baseado no consenso e na tecnologia, surge como paradigma capaz de equilibrar eficiência e garantias fundamentais[258] .

Outro aspecto relevante da cooperação internacional diz respeito à harmonização legislativa entre os países. A ausência de uniformidade na tipificação dos delitos e nas penas aplicáveis gera lacunas que beneficiam criminosos que exploram jurisdições mais brandas. A evolução do Direito Penal, conforme ressalta Tavares, depende de reformas estruturais que reconheçam a natureza tecnológica dos novos comportamentos delitivos[259] .

Os casos recentes de crimes de *phishing, ransomware* e estupro virtual demonstram como a cooperação jurídica internacional é indispensável para a responsabilização dos autores. Esses crimes frequentemente envolvem o uso de redes privadas, identidades falsas e hospedagens descentralizadas, o que dificulta a investigação tradicional. O trabalho conjunto entre polícias cibernéticas e ministérios públicos de diferentes países tem se mostrado fundamental para romper o anonimato e garantir a punição efetiva[260] .

O fortalecimento da cooperação jurídica internacional deve ser compreendido como um imperativo estratégico para a proteção da ordem pública digital. A união entre Estados, órgãos de investigação e entidades privadas possibilita respostas mais rápidas, técnicas e proporcionais à complexidade do cibercrime. A construção de um modelo colaborativo global é, portanto, o caminho para assegurar que a justiça penal acompanhe o ritmo da transformação tecnológica e preserve sua legitimidade no século XXI[261] .

5.6 Conflitos de jurisdição em ambiente digital

A expansão das redes digitais e a globalização das comunicações criaram um cenário inédito de sobreposição de jurisdições, em que diversos Estados reivindicam competência para processar e punir um mesmo crime cibernético. Essa multiplicidade de ordens jurídicas decorre do caráter transnacional das infrações, que frequentemente envolvem autores, vítimas e servidores localizados em países distintos. O resultado é o surgimento de conflitos de jurisdição, exigindo que o Direito Penal e o Direito Internacional desenvolvam critérios objetivos de delimitação de competências[262] .

---

[258] GABRIEL, 2022, p. 41.
[259] TAVARES, 2012, p. 172.
[260] BARBOSA; CEZAR; CARVALHO, 2024, p. 11.
[261] FRAGA; VANGLLER, 2017, p. 212.
[262] SILVA, 2024, p. 14.

Um dos principais problemas práticos é a dupla incriminação, situação em que uma conduta pode ser enquadrada simultaneamente em legislações de diferentes países, com consequências processuais e penais distintas. Essa duplicidade gera insegurança jurídica e risco de violação ao princípio do ne bis in idem, que impede a punição múltipla pelo mesmo fato. Para mitigar esses conflitos, torna-se essencial a cooperação jurídica entre os Estados e a adoção de acordos bilaterais que definam regras claras sobre o exercício da jurisdição[263] .

A aplicação da lei penal no ciberespaço exige novos parâmetros de territorialidade. Como as ações ilícitas digitais não respeitam fronteiras físicas, o local de consumação do crime — o locus delicti — passa a ser determinado pela ocorrência dos efeitos lesivos. Assim, a competência pode ser reconhecida tanto no país de onde partiu a ação quanto naquele onde o dano foi sentido. Essa interpretação de ubiquidade busca compatibilizar a soberania estatal com a natureza global das condutas digitais[264] .

No Brasil, o Código de Processo Penal, ao tratar da cadeia de custódia digital, estabelece mecanismos para garantir a integridade e autenticidade das provas coletadas, mesmo quando obtidas em cooperação com outras jurisdições. Essa regulamentação visa reduzir disputas sobre a validade das evidências e assegurar que as informações provenientes do exterior mantenham valor probatório em território nacional[265] .

Os conflitos de jurisdição também se manifestam na relação entre autoridades nacionais e empresas estrangeiras que operam serviços digitais. As plataformas globais, muitas vezes sediadas em países com legislações de proteção de dados mais rígidas, recusam-se a atender ordens judiciais brasileiras, alegando limitação territorial. Essa resistência impõe barreiras ao cumprimento de decisões judiciais e à efetividade da persecução penal[266] .

Um dos critérios mais aceitos para resolver conflitos de jurisdição é o da preponderância do interesse lesado, ou seja, deve prevalecer a jurisdição do Estado mais afetado pelo crime. Nos delitos cibernéticos, isso pode ser aferido pela localização da vítima, do agente ou do servidor que processou os dados ilícitos. Essa lógica busca equilibrar eficiência investigativa e respeito à soberania, reduzindo o risco de disputas diplomáticas[267] .

A teoria da jurisdição funcional, aplicada em alguns sistemas internacionais, propõe que a competência deve ser determinada pela capacidade efetiva de cada Estado em investigar e

[263] PORTELA, 2025, p. 119.
[264] LÓSSIO, 2022, p. 103.
[265] BRASIL, 2022.
[266] COLAÇO, 2017, p. 7.
[267] COSTA; CRUZ, 2016, p. 5.

julgar o caso. Esse critério pragmático prioriza a resposta mais rápida e eficaz, ainda que implique concessões mútuas entre países. No contexto digital, essa abordagem tem se mostrado fundamental para enfrentar crimes que evoluem em tempo real, como fraudes eletrônicas e invasões de sistemas[268] .

Os conflitos jurisdicionais não são apenas de natureza territorial, mas também de ordem axiológica. Cada país possui diferentes compreensões sobre liberdade de expressão, privacidade e segurança, o que pode gerar divergências na qualificação penal de determinadas condutas. A harmonização normativa entre os Estados é, portanto, essencial para evitar disparidades de tratamento e consolidar uma política criminal globalmente coerente[269] .

A resolução dos conflitos de jurisdição no ambiente digital depende da conjugação entre critérios técnicos e princípios jurídicos universais. A cooperação internacional, aliada à adoção de parâmetros como localização da vítima e extensão do dano, pode proporcionar um equilíbrio entre eficiência punitiva e respeito à soberania. O futuro da jurisdição penal digital está na construção de um sistema global de responsabilização que una tecnologia, segurança e justiça[270].

5.7 O metaverso e os desafios para a jurisdição penal

O surgimento do metaverso — um ambiente virtual tridimensional, interativo e descentralizado — trouxe novos desafios à aplicação do Direito Penal. A dificuldade de delimitar o local da prática delitiva, a identidade dos agentes e a natureza das condutas cometidas em realidades imersivas coloca em xeque os parâmetros tradicionais de jurisdição. No metaverso, ações realizadas por meio de avatares e inteligências artificiais autônomas diluem as fronteiras entre o mundo físico e o digital, exigindo a reformulação das noções clássicas de território e responsabilidade penal[271]

A definição do *locus delicti* em um ambiente que não possui geografia física concreta representa uma das principais dificuldades para o Direito Penal contemporâneo. A doutrina brasileira ainda não consolidou critérios para identificar o local do crime quando o ato ocorre em um servidor estrangeiro ou em múltiplos nós de rede simultaneamente. Tal situação exige novas teorias de competência penal que levem em conta a ubiquidade tecnológica e a

[268] BARROSO, 2018, p. 259.
[269] PORTELA, 2025, p. 124.
[270] GOMES, 2024, p. 88.
[271] SILVA, 2024, p. 13.

descentralização da informação[272]

A ausência de fronteiras fixas no metaverso desafia o princípio da territorialidade e questiona a própria legitimidade da jurisdição estatal sobre ações digitais. O marco regulatório atual, como o Código de Processo Penal e o Marco Civil da Internet, ainda não contemplam de forma explícita essas realidades virtuais autônomas. Diante disso, torna-se imprescindível repensar as normas de conexão entre fatos e territórios, de modo a preservar a coerência do sistema penal[273] .

Além do problema da territorialidade, a identificação do agente em ambientes virtuais tridimensionais é um desafio técnico e jurídico. No metaverso, é possível utilizar avatares, criptografia e camadas de anonimato que tornam praticamente impossível rastrear o autor de um delito. Tal cenário exige a criação de mecanismos cooperativos de rastreamento digital, sem violar os direitos fundamentais à privacidade e à proteção de dados[274] .

A responsabilidade penal de condutas automatizadas também constitui um tema emergente. Inteligências artificiais que interagem de forma autônoma com outros usuários podem causar danos jurídicos sem intervenção humana direta. O debate sobre a imputação penal em casos como esses ainda está em estágio inicial, mas aponta para a necessidade de novos parâmetros dogmáticos capazes de distinguir a ação humana mediada pela tecnologia da ação autônoma da máquina[275] .

Nesse contexto, o metaverso desafia os fundamentos clássicos do Direito Penal ao questionar a própria natureza da conduta e do resultado. Se uma agressão simbólica ou sexual ocorre entre avatares, há ou não crime? A ausência de contato físico não exclui o dano psicológico, o que indica a urgência de reinterpretar os conceitos de bem jurídico tutelado e lesividade. A abordagem penal deve, portanto, expandir-se para considerar novas formas de violência digital[276] .

A questão da jurisdição no metaverso também demanda cooperação internacional, pois a descentralização das plataformas impede a vinculação exclusiva a um ordenamento jurídico. O estudo de Prestes e Anacleto demonstra que a cooperação penal deve evoluir para mecanismos de resposta ágil e técnica, adaptados à volatilidade dos espaços digitais. A construção de redes multilaterais de comunicação entre autoridades é, portanto, essencial para

[272] TAVARES, 2012, p. 178.
[273] BRASIL, 2022
[274] COLAÇO, 2017, p. 5.
[275] BARROSO, 2018, p. 265.
[276] FRUMI, 2022, p. 152.

enfrentar esses novos desafios[277] .

A teoria constitucional contemporânea propõe uma releitura da jurisdição à luz da pluralidade dos espaços normativos. No caso do metaverso, Barroso defende a prevalência de uma interpretação que preserve os direitos fundamentais e assegure a legitimidade da atuação estatal, ainda que em ambientes simulados. O poder punitivo deve ser exercido de forma proporcional e fundamentada, evitando-se o risco de intervenções arbitrárias em contextos de incerteza tecnológica[278] .

O metaverso representa uma nova fronteira para o Direito Penal e para a jurisdição. As dificuldades de localização, identificação e imputação demandam uma dogmática inovadora, pautada pela cooperação global e pela proteção dos direitos humanos digitais. O desafio reside em equilibrar a liberdade criativa das realidades virtuais com a necessidade de segurança jurídica, garantindo que a evolução tecnológica não se torne um refúgio para a impunidade[279] .

5.8 Propostas para uma jurisdição penal eficiente no combate ao cibercrime

O enfrentamento do cibercrime exige uma jurisdição penal capaz de acompanhar a velocidade das transformações tecnológicas. A estrutura tradicional, baseada em fronteiras físicas e processos burocráticos, mostra-se insuficiente diante da natureza global e instantânea das infrações digitais. A modernização institucional e a criação de núcleos especializados de cooperação tecnológica e jurídica representam caminhos estratégicos para aumentar a eficiência investigativa e processual no combate ao crime cibernético[280] .

Uma jurisdição penal eficiente deve ser sustentada pela integração entre os órgãos de persecução penal e as autoridades de tecnologia da informação. A criação de centros de resposta rápida e unidades especializadas em análise digital permitiria maior agilidade na coleta e preservação de provas, reduzindo a dependência de solicitações externas e agilizando a responsabilização dos agentes[281] .

Nesse contexto, o uso de inteligência artificial (IA) surge como um instrumento poderoso de aprimoramento processual. Sistemas de IA podem cruzar grandes volumes de dados, identificar padrões de comportamento e prever potenciais ameaças cibernéticas. No

[277] PRESTES; ANACLETO, 2024, p. 6.
[278] BARROSO, 2018, p. 271.
[279] SILVA, 2024, p. 19.
[280] SOUZA; CERVINSKI, 2021, p. 4.
[281] BRASIL, 2014

entanto, sua utilização deve respeitar os limites constitucionais e garantir a observância dos direitos fundamentais, evitando abusos no monitoramento e na interceptação de informações[282].

A segurança da informação é outro pilar essencial para a eficiência jurisdicional. A ausência de protocolos unificados para o tratamento de dados compromete a validade das provas e a integridade das investigações. A implementação de normas técnicas de criptografia, certificação digital e rastreabilidade deve ser prioridade para garantir a autenticidade dos elementos probatórios[283] .

A integração das bases de dados entre as instituições nacionais e internacionais é uma medida indispensável para fortalecer a cooperação. Essa prática permite o compartilhamento rápido de informações sobre suspeitos, incidentes e métodos de ataque, reduzindo o tempo de resposta e ampliando o alcance das ações de persecução penal. A interoperabilidade entre sistemas é, portanto, um elemento-chave de uma política criminal moderna[284]

A consolidação de políticas públicas voltadas à cibersegurança também se mostra urgente. Conforme destaca Berlanda, o avanço da Internet das Coisas (IoT) amplia a vulnerabilidade das redes e requer um aparato jurídico e técnico de proteção compatível com o volume de dispositivos conectados. A ausência de regulamentação específica fragiliza a capacidade estatal de prevenir e responder aos ataques[285] .

Além disso, a padronização legislativa internacional é condição essencial para evitar lacunas jurídicas exploradas por criminosos que operam em diferentes jurisdições. A harmonização de conceitos e penas, aliada à simplificação dos procedimentos de cooperação, permitirá maior previsibilidade e efetividade nas ações conjuntas entre Estados[286] .

A qualificação continuada dos profissionais do sistema de justiça é outro ponto central para a eficiência da jurisdição penal digital. Juízes, promotores e peritos devem ser capacitados em temas como análise forense, anonimato digital e funcionamento de redes descentralizadas. A formação técnica e interdisciplinar contribui para decisões mais fundamentadas e adequadas às novas realidades tecnológicas[287] .

A construção de uma jurisdição penal eficiente no combate ao cibercrime depende de um equilíbrio entre inovação tecnológica e garantismo jurídico. O avanço digital deve ser aliado da justiça, não instrumento de violação de direitos. Somente por meio da cooperação global, da

[282] GABRIEL, 2022, p. 27.
[283] ALEXANDRIA, 2009, p. 45.
[284] TEIXEIRA, 2024, p. 84.
[285] BERLANDA, 2021, p. 19.
[286] GOMES, 2023, p. 77.
[287] FRAGA; VANGLLER, 2017, p. 312.

modernização processual e do fortalecimento institucional será possível assegurar que o Direito Penal continue eficaz e legítimo em meio à complexidade do ciberespaço[288] .

6 Cibersegurança e a efetividade do direito penal

A crescente digitalização das relações sociais, econômicas e institucionais transformou o ciberespaço em um dos principais campos de vulnerabilidade contemporânea. Nesse cenário, a cibersegurança emerge como um elemento essencial não apenas de proteção tecnológica, mas de preservação da ordem jurídica e da efetividade penal. A interdependência entre sistemas digitais e atividades humanas amplia o potencial de riscos — desde fraudes financeiras e ataques de ransomware até crimes contra a honra e a intimidade — exigindo que o Direito Penal atue de forma estratégica, preventiva e articulada com as políticas de segurança da informação. A aplicação eficaz das normas penais passa a depender, portanto, da capacidade do Estado e das instituições privadas em assegurar a integridade, a confidencialidade e a disponibilidade dos dados digitais.

Ao mesmo tempo, o avanço das ameaças cibernéticas impõe a necessidade de integração entre o Direito Penal e a governança da segurança da informação, consolidando uma abordagem multidisciplinar. A prevenção e repressão aos delitos informáticos exigem não apenas normas

[288] BRASIL, 2014

punitivas, mas também estruturas de *compliance*, educação digital, protocolos de resposta e parcerias internacionais voltadas à cooperação técnica e investigativa. A cibersegurança, nesse contexto, não é apenas um instrumento tecnológico, mas um componente essencial da efetividade penal, garantindo que a lei acompanhe a velocidade da inovação e preserve os direitos fundamentais em meio à complexidade do mundo digital.

6.1 Principais ameaças cibernéticas e sua repercussão penal

A consolidação da sociedade digital trouxe avanços incontestáveis, mas também desencadeou um aumento expressivo de ameaças cibernéticas que desafiam os limites do Direito Penal. O ambiente virtual passou a abrigar condutas ilícitas sofisticadas, que se manifestam por meio de invasões a sistemas, manipulações de dados e fraudes de identidade digital. Dentre as principais modalidades destacam-se o *phishing, o ransomware,* os ataques de negação de serviço (DDoS), os *deepfakes* e as violações de dados pessoais. Essas práticas afetam não apenas a privacidade e o patrimônio, mas também a confiança social nos sistemas digitais, exigindo uma resposta jurídica mais ágil e adequada às novas formas de criminalidade. Nesse contexto, o Direito Penal enfrenta o desafio de equilibrar repressão e garantismo, assegurando que a persecução de condutas virtuais preserve os princípios da legalidade e da segurança jurídica[289] .

O phishing é uma das técnicas mais disseminadas entre os crimes cibernéticos. Consiste no envio de mensagens fraudulentas que simulam comunicações legítimas, com o objetivo de obter dados pessoais, bancários ou corporativos de forma ilícita. A partir dessa manipulação, o agente pode cometer crimes de estelionato, falsidade ideológica e até lavagem de dinheiro, dependendo do uso posterior das informações coletadas. Ainda que a fraude se realize por meio eletrônico, a materialidade do delito é inequívoca, pois há dolo e lesão patrimonial efetiva. O Código Penal e a Lei nº 12.737/2012 conferem base normativa para punir tais condutas, mas as rápidas transformações tecnológicas demandam atualização contínua do ordenamento jurídico, especialmente diante da internacionalização dos ataques e da dificuldade de rastreamento dos autores[290] .

Outro tipo de ameaça que ganhou grande repercussão penal é o *ransomware,* uma modalidade de ataque em que o agente invade o sistema da vítima, criptografa seus arquivos e exige pagamento de resgate para restabelecer o acesso. Essa prática se enquadra em crimes

[289] ARAÚJO, 2015, p. 22.
[290] COSTA; CRUZ, 2016, p. 11.

como extorsão, dano e invasão de dispositivo informático, conforme tipificado na Lei nº 12.737/2012. O uso de criptomoedas como meio de pagamento e o anonimato proporcionado pela rede tornam a investigação complexa, pois dificultam a rastreabilidade dos valores e a identificação dos responsáveis. Além disso, o impacto social do *ransomware* é significativo, pois muitas vezes paralisa serviços essenciais, afetando hospitais, bancos e órgãos públicos. Essa natureza difusa do dano reforça a importância de políticas de cibersegurança preventiva, aliadas à responsabilização penal dos autores[291] .

Os ataques de negação de serviço, conhecidos como DDoS (*Distributed Denial of Service)*, são igualmente preocupantes. Diferentemente de outras modalidades, eles não visam o acesso indevido a dados, mas a sobrecarga de servidores até que os sistemas se tornem inoperantes. Tais ataques comprometem a estabilidade de plataformas financeiras, governamentais e empresariais, configurando infrações contra a administração pública e a economia popular. No plano penal, podem ser enquadrados como crimes de interrupção de serviço de utilidade pública ou sabotagem digital, conforme a gravidade do resultado. O Estado, nesse sentido, tem o dever de fortalecer suas infraestruturas críticas, implementando sistemas de proteção e investigação compatíveis com a complexidade das ameaças distribuídas em rede[292] .

A emergência das *deepfakes* representa um novo marco nos debates sobre cibercriminalidade. Por meio de algoritmos de inteligência artificial, é possível criar vídeos, imagens e áudios falsos com aparência realista, capazes de destruir reputações, manipular eleições ou extorquir indivíduos. As implicações penais são amplas: dependendo do caso, a conduta pode configurar crimes contra a honra, falsidade documental, extorsão e até estupro virtual, quando o material envolve conteúdo sexual. Além da tipificação, há um desafio probatório substancial, pois as falsificações digitais dificultam a distinção entre real e simulado, comprometendo a autenticidade das provas judiciais. O Direito Penal precisa, portanto, incorporar mecanismos de perícia digital e estabelecer parâmetros claros para a admissibilidade de evidências produzidas em ambientes virtuais[293] .

As fraudes digitais, por sua vez, abrangem uma gama extensa de condutas ilícitas, como clonagem de cartões, falsificação de identidades, manipulação de boletos e invasão de contas bancárias. Essas práticas exploram tanto vulnerabilidades tecnológicas quanto falhas humanas, evidenciando que a prevenção deve envolver políticas de segurança cibernética integradas ao

[291] BRASIL, 2012
[292] ALEXANDRIA, 2009, p. 87.
[293] FRAGA; VANGLLER, 2017, p. 142.

sistema penal. O Brasil vem buscando adequar sua legislação às demandas contemporâneas, mas a execução das normas ainda enfrenta entraves técnicos e jurisdicionais. A efetividade da resposta penal depende da colaboração entre Estado, setor privado e provedores de serviços digitais, numa abordagem de governança compartilhada[294] .

A engenharia social desponta como um dos elementos centrais na origem da maioria dos crimes cibernéticos. Trata-se da manipulação psicológica das vítimas para induzi-las a realizar ações que comprometem a segurança de sistemas ou expõem dados sensíveis. O agente, ao explorar a confiança ou a falta de conhecimento técnico, consegue acesso indevido a informações confidenciais sem necessariamente empregar meios tecnológicos complexos. Essa modalidade, que mescla persuasão e fraude, evidencia a importância do fator humano na segurança digital. Sob a ótica penal, o comportamento pode ser enquadrado em delitos de estelionato, falsidade ou obtenção de vantagem ilícita, demonstrando que o crime cibernético nem sempre decorre de habilidade técnica, mas da exploração de fragilidades cognitivas[295] .

O fator humano, aliás, é reconhecido como o elo mais vulnerável da cadeia de segurança cibernética. A ausência de treinamento adequado, a negligência na proteção de senhas e o uso indevido de dispositivos corporativos contribuem para a ocorrência de delitos digitais. Por isso, a cibersegurança não deve ser tratada apenas como responsabilidade técnica, mas também como questão de cultura organizacional e de dever jurídico. Políticas institucionais que promovam a conscientização dos usuários e a responsabilidade compartilhada são complementares ao Direito Penal, funcionando como instrumentos preventivos indispensáveis[296] .

Assim, as principais ameaças cibernéticas e suas repercussões penais demonstram a urgência de um sistema jurídico mais dinâmico e interligado às práticas tecnológicas. O enfrentamento do cibercrime requer tanto o fortalecimento das normas repressivas quanto a criação de ambientes digitais mais seguros, com ênfase na prevenção, cooperação internacional e capacitação técnica. O Direito Penal, ao lidar com essas novas formas de criminalidade, precisa manter-se fiel ao princípio da legalidade, garantindo previsibilidade e proporcionalidade nas sanções, sem perder de vista a necessidade de proteção eficaz dos bens jurídicos na era digital[297] .

A Internet das Coisas (IoT) ampliou a superfície de ataque com bilhões de dispositivos pouco seguros, criando vetores para *botnets*, espionagem e sabotagem remota. A exploração de

[294] BERLANDA, 2021, p. 19.
[295] COSTA; CRUZ, 2016, p. 12.
[296] SILVA; COSTA, 2023, p. 7.
[297] ARAÚJO, 2015, p. 25.

firmwares desatualizados e credenciais padrão permite desde DDoS massivos até invasões a ambientes industriais, com repercussões penais que vão de crimes contra a inviolabilidade de sistemas a perigo comum qualificado. A resposta jurídica precisa contemplar deveres mínimos de segurança por fabricantes e administradores de redes, sob pena de responsabilização por omissão relevante em cenários de risco previsível[298] .

A exposição de dados pessoais decorrente de violações de segurança não é apenas um incidente tecnológico, mas um fato juridicamente relevante que pode caracterizar crimes como receptação de dados, fraudes e extorsões, a depender do uso subsequente das informações. O elemento subjetivo mostra-se evidente quando o agente se vale de falhas humanas e técnicas para obter vantagem ilícita, exigindo perícia forense robusta e cadeia de custódia íntegra para a validade probatória. Daí a importância de políticas de minimização de dados, registro de logs e planos de resposta a incidentes como medidas de redução do dano penal[299] .

A efetividade da persecução penal diante de ameaças complexas pressupõe *readiness* institucional: inventários precisos de ativos, segmentação de redes, exercícios de mesa e integração entre segurança da informação e jurídico. Esses requisitos organizacionais impactam diretamente a preservação de vestígios digitais, a identificação do modus operandi e a correlação entre eventos técnicos e tipos penais, fortalecendo a prova e encurtando o ciclo de detecção-resposta. Em termos de governança, auditorias periódicas e métricas de maturidade permitem alinhar defesa técnica à tutela penal dos bens jurídicos afetados[300] .

6.2 Técnicas de proteção, compliance e políticas de segurança

A proteção de dados e a segurança cibernética assumiram papel central nas estratégias institucionais contemporâneas, especialmente em um cenário em que a informação se tornou ativo econômico e jurídico. Empresas públicas e privadas, bem como órgãos estatais, passaram a reconhecer que a gestão de riscos digitais ultrapassa o âmbito técnico e alcança o campo jurídico e penal. Nesse contexto, surgem os programas de *compliance* digital, voltados para a prevenção de ilícitos e a construção de uma cultura organizacional baseada em ética, responsabilidade e transparência. O *compliance* funciona como uma barreira preventiva contra condutas criminosas, mitigando a responsabilidade penal da pessoa jurídica e reforçando a

[298] BERLANDA, 2021, p. 27.
[299] SILVA; COSTA, 2023, p. 8.
[300] ALEXANDRIA, 2009, p. 93.

integridade institucional[301] .

O *compliance* digital representa, portanto, uma evolução das políticas tradicionais de governança corporativa. Ele busca alinhar práticas empresariais às exigências legais sobre proteção de dados, crimes informáticos e responsabilidade civil. A aplicação dessas normas exige auditorias periódicas, relatórios de vulnerabilidade e treinamentos internos, que permitem às organizações responder de forma rápida a incidentes de segurança. Além disso, a adoção de programas formais de integridade digital demonstra ao Poder Público a boa-fé da instituição em evitar ilícitos, podendo reduzir penalidades em casos de investigação ou responsabilização[302] .

A responsabilidade institucional também se estende às políticas internas de segurança da informação. Essas políticas, quando bem estruturadas, estabelecem normas claras de acesso, uso e armazenamento de dados, criando uma cultura de segurança coletiva. O Marco Civil da Internet, ao determinar deveres de guarda e sigilo aos provedores, reforça que o setor privado desempenha papel essencial na prevenção e repressão de ilícitos digitais. Assim, a cooperação entre empresas e autoridades se torna eixo fundamental para garantir a efetividade da lei penal em ambiente virtual[303] .

A perspectiva constitucional do tema também é indispensável, pois a proteção da privacidade, da intimidade e dos dados pessoais é um desdobramento direto dos direitos fundamentais. O artigo 5º da Constituição Federal assegura a inviolabilidade das comunicações e a proteção da vida privada, impondo ao Estado e às organizações o dever de zelar por essas garantias. A partir desse fundamento, políticas de segurança corporativa não podem ser tratadas apenas como exigência técnica, mas como expressão da dignidade humana e da cidadania digital. A governança institucional deve, portanto, equilibrar liberdade informacional e responsabilidade penal[304] .

O desenvolvimento de políticas de *compliance* digital requer ainda uma compreensão transnacional, já que os fluxos de dados e as infraestruturas de rede são globalizados. As organizações que operam em diversos países precisam atender simultaneamente a legislações diferentes, como a Lei Geral de Proteção de Dados brasileira e o Regulamento Europeu de Proteção de Dados (GDPR). Nesse cenário, o Direito Internacional Público assume papel mediador, promovendo a cooperação entre jurisdições e a harmonização de normas para

[301] BRITO, 2017, p. 64.
[302] FRUMI, 2022, p. 148.
[303] COLAÇO, 2017, p. 10.
[304] BARROSO, 2018, p. 317.

enfrentar crimes digitais e violações transfronteiriças[305] .

Além do aspecto jurídico, há um componente humano decisivo na efetividade das políticas de segurança. Conforme ressalta Mitnick (2003), o elo mais vulnerável da cadeia digital é o próprio usuário, e a maioria dos ataques ocorre devido à manipulação psicológica, negligência ou desconhecimento. Programas de *compliance* bem-sucedidos, portanto, investem em educação e conscientização contínua, promovendo treinamentos e simulados de resposta a incidentes. Ao transformar a segurança em valor institucional, as organizações reduzem riscos e fortalecem a cultura de prevenção[306].

Os provedores de serviços de internet e plataformas digitais têm papel relevante nesse ecossistema de governança. Como intermediários do tráfego informacional, assumem obrigações específicas quanto à guarda de registros e à colaboração com investigações penais. A jurisprudência brasileira tem reconhecido a responsabilidade subsidiária desses agentes quando omissos na adoção de medidas preventivas. Essa corresponsabilidade técnica e jurídica reforça a importância de políticas internas alinhadas à legislação penal e civil, sobretudo no combate a fraudes, difamações e crimes contra a honra praticados em rede[307] .

A governança corporativa, quando aplicada ao contexto da cibersegurança, também se torna instrumento de responsabilidade social. Instituições que adotam mecanismos de controle interno e transparência na gestão de dados contribuem para a construção de um ambiente digital mais confiável e ético. O fortalecimento das políticas de *compliance* é, portanto, uma medida não apenas de autoproteção, mas de compromisso com o Estado Democrático de Direito. Nesse sentido, a cultura de integridade deve ser integrada à estratégia institucional como um valor perene e não apenas como resposta a exigências regulatórias[308].

As técnicas de proteção, o *compliance* digital e as políticas de segurança convergem para um mesmo objetivo: a efetividade da prevenção penal e a proteção da sociedade frente aos riscos tecnológicos. O Direito Penal, por sua vez, deve reconhecer e incentivar essas práticas, integrando-as ao seu sistema repressivo e educativo. A cibersegurança institucional precisa ser tratada como política pública e empresarial permanente, sustentada em princípios constitucionais, parâmetros internacionais e diretrizes éticas. Somente assim será possível garantir uma governança digital que una segurança, legalidade e respeito aos direitos fundamentais[309] .

---

[305] PORTELA, 2025, p. 201.
[306] MITNICK; SIMON, 2003, p. 42.
[307] LEONARDI, 2005, p. 89.
[308] BRITO, 2017, p. 66.
[309] BARROSO, 2018, p. 322.

A incorporação de cláusulas de segurança e privacidade em contratos com provedores e parceiros, somada a due diligence técnica e jurídica, integra o núcleo do compliance digital. Para além de políticas internas, é crucial definir responsabilidades na guarda de registros, prazos de retenção e fluxos de atendimento a ordens judiciais, sob pena de imputações por omissão culposa. A literatura sobre provedores destaca que a governança contratual bem desenhada reduz litígios e qualifica a cooperação com autoridades[310] .

No plano transnacional, programas de compliance precisam mapear conflitos de lei e obrigações concorrentes de sigilo e de cooperação, adotando cláusulas de data residency, avaliação de impacto e mecanismos de transferência internacional de dados. Esse desenho jurídico-técnico mitiga riscos penais decorrentes de descumprimento de ordens estrangeiras ou de violação de garantias locais, favorecendo uma postura de cooperação que respeite soberania e devido processo legal[311] .

Do ângulo constitucional, compliance e políticas de segurança devem ser calibrados pela proporcionalidade, evitando medidas intrusivas desnecessárias que convertam o ambiente corporativo em espaço de vigilância excessiva. Treinamentos, controles de acesso e monitoração devem ser adequados, necessários e proporcionais à finalidade de proteção, preservando a dignidade e a privacidade dos trabalhadores — condição que fortalece a legitimidade das práticas e sua defesa em juízo[312] .

6.3 Legislação nacional e internacional sobre cibersegurança

A expansão das tecnologias digitais e o aumento da criminalidade cibernética exigiram do Direito Penal uma resposta mais estruturada e integrada, tanto em nível nacional quanto internacional. No Brasil, o Marco Civil da Internet (Lei nº 12.965/2014) consolidou princípios fundamentais para o uso responsável da rede, estabelecendo direitos e deveres para usuários, provedores e o próprio Estado. Ele introduziu conceitos essenciais de neutralidade da rede, privacidade e responsabilidade na guarda de dados, criando a base jurídica para o desenvolvimento da cibersegurança nacional. No entanto, a complexidade dos crimes digitais demanda uma legislação mais específica e adaptável, capaz de acompanhar a velocidade das inovações tecnológicas e suas consequências jurídicas[313] .

---

[310] LEONARDI, 2005, p. 101.
[311] PORTELA, 2025, p. 205.
[312] BARROSO, 2018, p. 320.
[313] BRASIL, 2014

Em complemento, a Lei nº 12.735/2012 determinou que órgãos públicos criassem delegacias e setores especializados em crimes cibernéticos, reconhecendo oficialmente o impacto crescente desses delitos. Essa norma foi responsável por reforçar a estrutura investigativa do Estado e por estabelecer parâmetros iniciais de repressão penal a condutas realizadas no ambiente digital, como invasões de sistemas e disseminação de vírus. Ainda que importante, a aplicação dessa lei tem se mostrado limitada diante da natureza transnacional de muitos ataques, que extrapolam as fronteiras jurisdicionais e desafiam os mecanismos de persecução criminal tradicionais[314] .

Outro marco relevante é a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), que se articula diretamente com o Marco Civil e amplia as garantias de privacidade, impondo obrigações mais rigorosas às empresas e instituições públicas na coleta, tratamento e armazenamento de informações pessoais. Essa lei incorporou o princípio da responsabilização proativa, pelo qual o agente deve não apenas reparar danos, mas também demonstrar que adota medidas de segurança adequadas. O descumprimento dessas obrigações pode gerar responsabilização administrativa, civil e até penal, especialmente em casos de dolo ou negligência grave[315]

No campo penal, entretanto, ainda existem lacunas quanto à definição e à punição de condutas cibernéticas complexas. A legislação brasileira tipifica a invasão de dispositivos informáticos, mas enfrenta dificuldades em abarcar crimes emergentes, como o uso de *deepfakes* para fins de difamação ou fraude, e o sequestro de dados (*ransomware*). Essa defasagem entre inovação tecnológica e normatização jurídica é recorrente em diversos países e demonstra a urgência de uma harmonização legislativa internacional que assegure coerência e eficácia punitiva. O Brasil, nesse sentido, tem buscado alinhar-se a padrões globais, ainda que sem adesão formal a tratados internacionais como a Convenção de Budapeste[316] .

A responsabilidade dos provedores de serviço também é um ponto central no debate sobre cibersegurança e legislação penal. Conforme analisado por Leonardi, a responsabilidade civil e penal dessas empresas deve equilibrar a liberdade de expressão com a proteção dos direitos fundamentais, garantindo que a atuação digital não sirva de escudo para práticas ilícitas. O Marco Civil prevê que os provedores somente respondem por danos causados por terceiros após o descumprimento de ordens judiciais, princípio que visa evitar censura prévia e preservar

[314] CUNHA; CORTIZO, 2024, p. 4.
[315] MAIA; COSTA, 2023, p. 114.
[316] HERNANDEZ; TOLEDO, 2021, p. 77.

a neutralidade da rede. Ainda assim, em casos de omissão deliberada ou negligência na proteção de dados, é possível configurar responsabilidade compartilhada[317] .

No âmbito internacional, há um esforço crescente para estabelecer padrões mínimos de segurança digital e de responsabilização penal. Diversos países têm aprovado leis específicas sobre crimes cibernéticos e proteção de dados, inspiradas em modelos europeus e norte-americanos. Essas normas buscam uniformizar procedimentos de investigação, facilitar a cooperação entre autoridades e promover a troca segura de informações digitais. A criação de mecanismos multilaterais de controle, como grupos de trabalho em ciberdefesa e observatórios de crimes digitais, reflete a tendência global de tratar o ciberespaço como um território jurídico compartilhado[318] .

A integração entre o Direito Penal e o Direito Internacional é fundamental para combater crimes que atravessam fronteiras digitais. A descentralização das redes e o anonimato dificultam a identificação dos autores, exigindo acordos bilaterais e multilaterais de cooperação jurídica. Países que já possuem tratados consolidados demonstram maior agilidade nas respostas investigativas e judiciais, enquanto os sistemas nacionais que ainda operam de forma isolada enfrentam impunidade crescente. Essa articulação internacional é, portanto, condição necessária para a eficácia do Direito Penal no combate à criminalidade digital[319]

A legislação de cibersegurança também enfrenta o desafio de harmonizar princípios constitucionais — como legalidade, proporcionalidade e devido processo — com a urgência de respostas tecnológicas imediatas. Como destaca Barroso, o avanço normativo não pode comprometer direitos fundamentais sob o pretexto de segurança, devendo preservar o equilíbrio entre repressão penal e proteção das liberdades individuais. A eficácia normativa deve ser acompanhada de garantias processuais sólidas, sob pena de instaurar um sistema penal de exceção no ambiente digital[320]

A consolidação de uma legislação nacional e internacional sobre cibersegurança requer um modelo de governança global, baseado em cooperação, transparência e respeito à soberania dos Estados. O Direito Penal precisa assumir papel estratégico nesse processo, articulando-se com normas administrativas e civis para formar um sistema integrado de prevenção e repressão. A convergência entre tecnologia, direito e ética é o caminho mais seguro para garantir que o progresso digital não se converta em instrumento de vulnerabilidade, mas em espaço de

[317] LEONARDI, 2005, p. 93.
[318] PORTELA, 2025, p. 202.
[319] COLAÇO, 2017, p. 12.
[320] BARROSO, 2018, p. 318.

proteção e fortalecimento da cidadania digital[321]

A experiência comparada revela que a evolução normativa sobre cibersegurança é incremental e responsiva a incidentes de grande impacto, o que produz janelas de defasagem entre inovação e regulação. Para reduzir esse hiato, instrumentos de soft law, guias de boas práticas e normas técnicas podem servir de parâmetro de diligência, influenciando a interpretação penal sobre culpa e previsibilidade do risco, sem comprometer o núcleo do princípio da legalidade[322]

A cooperação internacional eficaz demanda tipificações minimamente convergentes e canais céleres de auxílio, mas também salvaguardas contra excessos punitivos. Modelos de assistência jurídica que preservem contraditório, publicidade mitigada e controle judicial reforçam a confiabilidade das provas digitais obtidas no exterior, evitando nulidades e consolidando um padrão probatório compartilhado entre jurisdições[323]

O equilíbrio entre segurança e liberdade exige que deveres de guarda, revelação e retirada de conteúdo sejam normativamente claros, com critérios de necessidade e prazos definidos. A adoção de métricas de accountability e logs auditáveis pelos provedores densifica a responsabilização sem descambar para censura prévia, harmonizando defesa social com a arquitetura de direitos fundamentais no ambiente digital[324]

6.4 Segurança em diferentes contextos digitais e institucionais

A segurança da informação, quando observada em diferentes contextos digitais e institucionais, revela uma complexa rede de vulnerabilidades e responsabilidades jurídicas. Órgãos públicos, empresas privadas e instituições financeiras operam com níveis distintos de exposição a riscos cibernéticos, o que demanda estratégias específicas de proteção e resposta. Nos setores governamentais, a fragilidade de sistemas e a dependência de tecnologias terceirizadas tornam os dados públicos especialmente suscetíveis a ataques de espionagem, sabotagem ou vazamento. A ausência de protocolos unificados de segurança e a defasagem tecnológica ampliam o potencial de prejuízos administrativos e penais, especialmente quando informações sigilosas são comprometidas[325]

No âmbito empresarial, a cibersegurança está diretamente ligada à integridade das

[321] CUNHA; CORTIZO, 2024, p. 16.
[322] HERNANDEZ; TOLEDO, 2021, p. 79.
[323] PORTELA, 2025, p. 209.
[324] BARROSO, 2018, p. 318.
[325] ALEXANDRIA; MARCIANO, 2006, p. 43.

operações corporativas e à reputação institucional. Empresas privadas, especialmente as que atuam em comércio eletrônico e tecnologia, são alvos frequentes de ataques de *phishing*, *ransomware* e *deepfakes*. Esses incidentes podem gerar prejuízos milionários, perda de propriedade intelectual e quebra de confiança entre consumidores e marcas. A responsabilidade penal das corporações, nesses casos, decorre tanto de ações dolosas quanto de omissões, como a falta de investimentos adequados em segurança ou o descumprimento da Lei Geral de Proteção de Dados. O impacto jurídico vai além da indenização civil, alcançando esferas criminais e administrativas[326].

Nas instituições financeiras, a segurança digital assume dimensão ainda mais crítica, pois envolve o fluxo constante de recursos e dados sensíveis. Ataques cibernéticos nesse setor afetam diretamente a economia e a estabilidade social, sendo considerados de alta relevância penal. Fraudes eletrônicas, invasões de contas e manipulações de sistemas de pagamento são condutas previstas em diversas tipificações, como a Lei nº 12.737/2012, que criminaliza a invasão de dispositivos informáticos. A responsabilização penal se estende aos agentes internos que facilitam ou negligenciam a segurança digital, reforçando a importância da supervisão contínua e da implementação de protocolos de rastreamento de transações[327].

No setor público, os riscos cibernéticos estão frequentemente associados à vulnerabilidade das infraestruturas críticas, como sistemas de saúde, segurança e energia. Um ataque direcionado a esses ambientes pode comprometer serviços essenciais e afetar diretamente os direitos fundamentais dos cidadãos. A legislação brasileira, ainda que reconheça a gravidade dessas ameaças, carece de normas específicas voltadas à proteção de dados governamentais. A ausência de uma cultura consolidada de cibersegurança nas instituições estatais fragiliza a capacidade de resposta e aumenta a dependência de mecanismos reativos, como investigações e auditorias pós-incidente[328].

Nas corporações privadas, o desafio está na integração entre tecnologia e governança. A implementação de políticas internas de segurança da informação, auditorias regulares e programas de *compliance* digital é indispensável para garantir a conformidade legal e reduzir vulnerabilidades. O descumprimento dessas obrigações pode configurar negligência penal, especialmente quando a omissão resulta em danos coletivos ou violações de dados pessoais. O

---

[326] VANDEREI, Matheus Luiz. Políticas públicas para combater crimes virtuais: insuficiência da Lei Geral de Proteção de Dados e adaptações necessárias à regulamentação setorial. Trabalho de Conclusão de Curso (Bacharelado em Direito)-Faculdade Nacional de Direito, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2024. p. 9

[327] BRASIL, 2012

[328] SOUZA; CERVINSKI, 2021, p. 7.

Direito Penal, nesse contexto, atua não apenas de forma repressiva, mas também preventiva, incentivando práticas empresariais éticas e responsáveis[329].

As instituições financeiras e de crédito, por lidarem com informações de alta sensibilidade, necessitam de protocolos de segurança mais rigorosos. A criptografia de dados, a autenticação multifatorial e o monitoramento constante de transações são mecanismos essenciais de defesa. Contudo, mesmo com tecnologias avançadas, o fator humano continua sendo a principal vulnerabilidade. Casos de engenharia social, em que funcionários são induzidos a conceder acesso a sistemas, demonstram que o fortalecimento da segurança institucional depende tanto da tecnologia quanto da capacitação dos profissionais envolvidos[330].

Em paralelo, cresce o debate sobre a responsabilização penal de gestores e executivos diante de falhas em sistemas de proteção digital. A omissão na adoção de medidas de segurança adequadas pode configurar culpa ou dolo eventual, sobretudo quando há consciência dos riscos. Essa responsabilização pessoal reforça a necessidade de que as políticas institucionais de segurança sejam incorporadas à rotina administrativa, com monitoramento constante e relatórios de conformidade documentados. O desafio está em equilibrar eficiência técnica com rigor jurídico, assegurando que a cibersegurança não se restrinja a um discurso corporativo, mas se traduza em práticas efetivas de proteção[331].

A criação de políticas públicas voltadas à segurança digital também é essencial para garantir que os diferentes contextos institucionais estejam amparados por um sistema jurídico integrado. A ausência de regulamentação setorial unificada gera insegurança jurídica e dificulta a cooperação entre órgãos e empresas. É necessário que o Estado promova mecanismos de certificação, auditoria e transparência, estimulando uma cultura de prevenção e de responsabilização compartilhada. Dessa forma, a governança da cibersegurança torna-se uma política de Estado, e não apenas uma preocupação individual de cada instituição[332].

Observa-se que a segurança digital em ambientes públicos e privados está intrinsecamente ligada à efetividade do Direito Penal e à proteção da cidadania digital. A ausência de preparo técnico, de políticas robustas e de normativas claras favorece a impunidade e enfraquece o controle sobre as infrações cibernéticas. O fortalecimento institucional, aliado à harmonização legislativa e à capacitação contínua dos agentes públicos e privados, é o caminho

---

[329] GABRIEL, 2022, p. 112.
[330] SANTIAGO, Anna Beatriz Vilhena; PICANÇO, Sarah Ruth Gondim; DIAS, Jean Carlos. A responsabilidade civil na ocorrência de exposição de crianças e adolescentes na internet. Revista Jurídica do Cesupa, v. 5, n. 1, p. 10-32, 2024. p. 22
[331] ALVES et al., 2024, p. 3.
[332] VANDEREI, 2024, p. 11

para uma segurança digital sólida e inclusiva. Nesse sentido, o Direito deve assumir papel ativo, articulando-se com a tecnologia para garantir justiça, responsabilidade e proteção no espaço virtual[333].

Em ambientes educacionais e sociais frequentados por crianças e adolescentes, políticas de segurança exigem camadas adicionais de proteção, como controle parental, moderação ativa e respostas rápidas a denúncias. A omissão institucional diante de exposições indevidas pode gerar responsabilização, impondo deveres específicos de prevenção, acolhimento e preservação de evidências para futura persecução penal[334].

No setor público, a tipificação de condutas de invasão e dano a sistemas, somada à estruturação de unidades especializadas, cria condições para responsabilização de agentes internos e externos, inclusive por falhas grosseiras de custódia da informação. A adoção de normas de segurança por padrão e por defeito reduz a incidência de incidentes e fortalece a legitimidade da atuação estatal em serviços críticos[335].

Estratégias setoriais de prevenção comprovam que campanhas de alfabetização digital, simulações periódicas e protocolos de reporte elevam a resiliência institucional e diminuem a janela de oportunidade criminosa. Ao internalizar essas práticas como política contínua, organizações públicas e privadas reduzem a exposição a fraudes e extorsões, ao mesmo tempo em que qualificam a produção de prova técnica para fins penais[336].

6.5 O fator humano e os riscos da engenharia social

O fator humano é, indiscutivelmente, o elo mais vulnerável da cadeia de segurança digital. Apesar dos avanços tecnológicos e da sofisticação dos sistemas de proteção, a maior parte dos ataques cibernéticos ainda depende da manipulação psicológica das vítimas — fenômeno conhecido como engenharia social. Trata-se de uma técnica criminosa baseada no engano e na exploração da confiança humana, utilizada para induzir pessoas a revelar informações sigilosas, clicar em links maliciosos ou conceder acessos indevidos. Essa vulnerabilidade humana, quando não tratada com políticas educativas e preventivas, transforma o indivíduo em porta de entrada para fraudes e crimes virtuais[337].

A engenharia social se manifesta de várias formas, como *phishing*, *spear phishing*,

[333] GABRIEL, 2022, p. 118.
[334] SANTIAGO; PICANÇO; DIAS, 2024, p. 24.
[335] BRASIL, 2012
[336] SOUZA; CERVINSKI, 2021, p. 9.
[337] MITNICK; SIMON, 2003, p. 41.

vishing, *baiting* e até mesmo falsas comunicações corporativas. Em todos os casos, o sucesso do ataque depende menos da capacidade técnica do criminoso e mais da habilidade em manipular o comportamento humano. Essa característica torna a prevenção um desafio não apenas tecnológico, mas também ético e pedagógico. O Direito Penal, nesse contexto, precisa reconhecer a relevância da conduta humana na cadeia causal do crime, avaliando quando a imprudência, negligência ou imperícia podem configurar responsabilidade penal[338].

A legislação brasileira tem evoluído no sentido de reconhecer a importância da segurança da informação como dever jurídico. A Lei nº 12.735/2012 prevê a criação de delegacias especializadas e reforça o papel das instituições na prevenção de crimes cibernéticos. Entretanto, ela não aborda de forma direta a dimensão humana desses delitos. Ainda que os sistemas de defesa digital sejam robustos, a falha humana pode neutralizar qualquer mecanismo de proteção, demonstrando que a segurança efetiva depende tanto da tecnologia quanto da conscientização dos usuários[339].

Nos ambientes corporativos, a negligência humana é uma das principais causas de incidentes de segurança. Funcionários que reutilizam senhas, compartilham acessos ou clicam em anexos suspeitos acabam contribuindo, ainda que involuntariamente, para a ocorrência de crimes. A ausência de treinamentos regulares e de políticas de *compliance* digital agrava esse quadro, uma vez que as empresas deixam de cumprir o dever de cuidado necessário para prevenir violações. Nesses casos, a responsabilidade pode alcançar tanto o indivíduo quanto a instituição, especialmente quando há omissão na implementação de medidas preventivas[340].

A doutrina penal moderna tem destacado que a culpa por negligência digital não se limita ao indivíduo comum, mas pode abranger gestores e profissionais de tecnologia que, por dever funcional, deveriam prever e evitar riscos previsíveis. A omissão dolosa ou culposa no tratamento de vulnerabilidades pode gerar responsabilização por conivência ou facilitação indireta do crime. Assim, o fator humano deve ser analisado não apenas sob a ótica da vítima, mas também sob a perspectiva do agente responsável pela segurança do sistema[341].

Do ponto de vista psicológico, a engenharia social aproveita-se de traços universais do comportamento humano, como a confiança, o medo e a curiosidade. Estudos apontam que campanhas de conscientização reduzem significativamente o número de incidentes, mas sua eficácia depende de constância e da criação de uma cultura organizacional voltada à segurança.

---

[338] FRAGA; VANGLLER, 2017, p. 72.
[339] BRASIL, 2012
[340] SILVA; COSTA, 2023, p. 5.
[341] MAIA; COSTA, 2023, p. 114.

Essa abordagem preventiva é mais eficaz do que a mera punição, pois atua antes da ocorrência do crime e reduz a vulnerabilidade coletiva[342].

Em termos jurídicos, a falha humana pode gerar diferentes tipos de responsabilização, variando conforme o contexto. No caso de servidores públicos, a negligência na proteção de dados pode configurar improbidade administrativa ou violação de sigilo funcional. Em empresas privadas, pode caracterizar violação contratual ou infração penal, conforme a gravidade do dano. Em ambos os casos, o dever de cuidado assume natureza objetiva, exigindo que todos os agentes que lidam com informações sigilosas adotem padrões mínimos de segurança e conduta ética[343].

A exposição de informações pessoais por descuido humano tem repercussões ainda mais graves quando envolve populações vulneráveis, como crianças e adolescentes. Casos de *cyberbullying*, vazamento de imagens e fraudes em redes sociais demonstram que a proteção digital vai além de mecanismos técnicos — ela depende da educação e da sensibilização social. O Estado, a família e as instituições têm o dever de orientar e fiscalizar o uso seguro da internet, sob pena de responderem civil e penalmente por omissões que causem danos a terceiros[344].

O combate à engenharia social requer uma estratégia integrada entre Direito, tecnologia e psicologia. É imprescindível reconhecer que o comportamento humano é o primeiro e o último elo da cadeia de segurança, sendo o treinamento contínuo e o fortalecimento da ética digital medidas indispensáveis. O Direito Penal deve atuar como garantidor da integridade das relações digitais, punindo condutas dolosas, mas também incentivando políticas educativas e preventivas. Assim, a construção de uma cultura de segurança informacional sólida depende do comprometimento coletivo e da responsabilização consciente de cada indivíduo conectado[345].

No âmbito corporativo, a engenharia social explora hierarquias e rotinas: pedidos falsos de urgência, imitação de executivos e golpes de suporte técnico têm alta taxa de sucesso quando não há verificação fora de banda. Programas de conscientização que treinam o "reflexo de suspeita" e instituem duplo controle para transações sensíveis reduzem significativamente o risco penal derivado de fraudes internas e externas[346].

A evolução tecnológica desloca o foco do atacante do perímetro para o comportamento: quanto mais seguras as camadas técnicas, maior o incentivo à manipulação humana. O Direito

[342] MITNICK; SIMON, 2003, p. 49.
[343] HERNANDEZ; TOLEDO, 2021, p. 80.
[344] SANTIAGO; PICANÇO; DIAS, 2024, p. 19.
[345] FRAGA; VANGLLER, 2017, p. 75.
[346] COSTA; CRUZ, 2016, p. 14.

Penal precisa, assim, distinguir com precisão a culpa pela quebra de protocolo do erro escusável, evitando imputações desmedidas e orientando sua intervenção à conduta dolosa e à omissão relevante diante de riscos notórios[347].

Quando as vítimas são hipervulneráveis, como crianças, adolescentes ou idosos, o dever de cuidado de plataformas, escolas e famílias ganha densidade jurídica. Processos de verificação, rotulagem de conteúdo e canais de denúncia acessíveis compõem uma política de proteção integral, cuja inobservância pode ensejar responsabilidades múltiplas, inclusive penais, diante de danos graves e previsíveis[348].

6.6 Cibersegurança, Direito Penal e o princípio da legalidade

A relação entre cibersegurança e Direito Penal apresenta desafios inéditos para a aplicação do princípio da legalidade, especialmente diante da velocidade das transformações tecnológicas. O avanço da inteligência artificial, da criptografia e das redes descentralizadas impõe novos tipos de condutas que não se enquadram facilmente nas tipificações tradicionais. Nesse cenário, o princípio da legalidade — segundo o qual não há crime sem lei anterior que o defina — atua como um freio essencial contra o arbítrio estatal, evitando que o poder punitivo extrapole os limites da norma escrita. A ciberdefesa, portanto, deve se equilibrar entre a necessidade de proteção coletiva e a preservação das garantias fundamentais do indivíduo[349].

O princípio da legalidade assume função garantista frente à inovação tecnológica, pois impede que interpretações extensivas ou analógicas sejam utilizadas para punir comportamentos não previstos em lei. No contexto digital, essa limitação é particularmente relevante, já que a natureza mutável das tecnologias tende a gerar zonas de incerteza jurídica. A tentação de ampliar conceitos penais para abarcar novas condutas, como fraudes virtuais e ataques cibernéticos complexos, pode resultar em violações de direitos, configurando punições desproporcionais e arbitrárias[350].

Contudo, a rigidez interpretativa do princípio da legalidade também não pode servir como pretexto para a ineficácia da tutela penal. A inexistência de normas claras sobre delitos informáticos cria um vácuo normativo que favorece a impunidade. Assim, a dogmática penal contemporânea precisa dialogar com a cibersegurança, reconhecendo a necessidade de atualizar

[347] HERNANDEZ; TOLEDO, 2021, p. 82.
[348] SANTIAGO; PICANÇO; DIAS, 2024, p. 26.
[349] BARROSO, 2018, p. 324.
[350] BRITO, 2017, p. 45.

os tipos penais e incluir condutas digitais que ameacem bens jurídicos relevantes, como a privacidade, a integridade de dados e a segurança das redes[351].

As legislações mais recentes, como o Marco Civil da Internet e a Lei nº 12.737/2012, representam avanços importantes na regulação das condutas digitais, mas ainda insuficientes para cobrir o espectro da criminalidade cibernética. O Marco Civil, ao estabelecer princípios de neutralidade, privacidade e responsabilização, fornece uma base normativa, porém não resolve o problema penal de condutas tecnológicas mais complexas. Por isso, a integração entre políticas de cibersegurança e legislação penal torna-se indispensável, a fim de garantir tanto a efetividade da punição quanto a segurança jurídica dos cidadãos[352].

A aplicação do princípio da legalidade no ciberespaço exige, portanto, um equilíbrio entre o formalismo da lei e a adaptação ao dinamismo digital. Para isso, é preciso adotar uma hermenêutica penal que preserve os direitos fundamentais, mas que também reconheça as novas formas de lesividade. A proporcionalidade, como princípio derivado da legalidade, deve orientar a criminalização das condutas digitais, evitando tanto a hiperpenalização quanto a omissão estatal. Essa diretriz permite que o Direito Penal atue de forma legítima, sem extrapolar sua função protetiva[353].

No plano internacional, o princípio da legalidade também é central para a harmonização das legislações sobre cibercrime. A multiplicidade de jurisdições e a ausência de uniformidade normativa dificultam a cooperação entre Estados, o que compromete a eficácia da repressão penal global. Para enfrentar esse problema, instrumentos de cooperação devem respeitar os limites constitucionais de cada país, evitando que a persecução transnacional resulte em violações de soberania ou de garantias processuais[354].

A responsabilidade penal dos provedores de internet e das plataformas digitais representa outro desafio relevante. A definição de suas obrigações de segurança e resposta diante de crimes cibernéticos precisa respeitar os limites da legalidade, evitando atribuições automáticas de culpa. A responsabilização deve estar ancorada em deveres objetivos previstos em lei, como os do Marco Civil, que delimitam o dever de guarda e de colaboração judicial. A ampliação indevida desses deveres sem base legal configura afronta direta ao princípio da legalidade penal[355].

Nesse contexto, o Direito Penal informático surge como campo indispensável para a

---

[351] CUNHA; CORTIZO, 2024, p. 6.
[352] FRUMI, 2022, p. 151.
[353] HERNANDEZ; TOLEDO, 2021, p. 81.
[354] PORTELA, 2025, p. 211.
[355] COLAÇO, 2017, p. 8.

construção de uma dogmática moderna, capaz de lidar com os fenômenos tecnológicos sem romper com os fundamentos clássicos. Auriney Brito destaca que a cibercriminalidade não exige apenas novas penas, mas uma reformulação de conceitos jurídicos, incluindo autoria, dolo e materialidade, para adequá-los à lógica digital. A modernização dogmática deve ocorrer dentro dos marcos legais e constitucionais, preservando o núcleo duro das garantias penais[356].

A cibersegurança e o princípio da legalidade devem ser compreendidos como pilares complementares de uma justiça penal contemporânea. Enquanto a cibersegurança protege a sociedade contra ameaças tecnológicas, a legalidade assegura que essa proteção ocorra dentro dos limites éticos e jurídicos do Estado de Direito. A interação entre ambos os campos deve buscar a proporcionalidade e a racionalidade punitiva, garantindo que o avanço digital seja acompanhado por um sistema penal justo, transparente e tecnicamente atualizado[357].

A delimitação legal dos deveres de guarda e colaboração dos provedores constitui cláusula de segurança jurídica: sem lei clara, o alargamento por analogia viola a legalidade e fragiliza a confiabilidade do ecossistema digital. O Marco Civil, ao positivar critérios objetivos, oferece balizas que evitam tanto a impunidade quanto a responsabilização automática e desproporcional[358].

A responsabilidade de intermediários informacionais, quando existente, deve ancorar-se em condutas típicas de descumprimento de deveres legais e ordens judiciais, não em presunções gerais de vigilância. Tal desenho protege a liberdade de expressão e reduz incentivos à remoção excessiva de conteúdos lícitos, preservando a coerência entre legalidade penal e arquitetura aberta da rede[359].

No cenário transfronteiriço, a legalidade cumpre papel de linguagem comum: tipificações claras e procedimentos previsíveis viabilizam cooperação, admissão de provas e execução de decisões, sem abdicar de garantias nacionais. Harmonização mínima e cláusulas de salvaguarda processual formam o núcleo de um modelo de ciberdefesa penal compatível com o Estado de Direito[360].

---

[356] BRITO, 2017, p. 52.
[357] MAIA; COSTA, 2023, p. 121.
[358] FRUMI, 2022, p. 153.
[359] COLAÇO, 2017, p. 11.
[360] PORTELA, 2025, p. 213.

7 Considerações Finais

As questões formuladas na delimitação do problema foram enfrentadas a partir da tensão central entre inovação tecnológica e garantias penais. Demonstrou-se que é possível aplicar a tipicidade penal a comportamentos em ambientes imersivos sem violar a legalidade, desde que a análise siga parâmetros objetivos e verificáveis. O percurso adotado confirmou que a proteção de bens jurídicos no ciberespaço exige rigor metodológico, sob pena de insegurança jurídica e expansão indevida do poder punitivo.

A presente dissertação teve como primeiro objetivo específico examinar a aplicabilidade dos tipos penais clássicos às condutas praticadas em meios digitais, avaliando sua adequação diante da criminalidade cibernética contemporânea. A análise desenvolvida ao longo do trabalho demonstrou que, embora alguns delitos tradicionais possam ser aplicados ao ambiente virtual por meio de interpretação sistemática, essa solução revela-se limitada e, em muitos casos, insuficiente. A transposição de tipos concebidos para a realidade física para o

ciberespaço gera insegurança jurídica, sobretudo quando se recorre a interpretações extensivas que tensionam o princípio da legalidade. Assim, constatou-se que a dogmática penal tradicional enfrenta dificuldades estruturais para abarcar condutas digitais complexas, marcadas pela desmaterialização, pela transnacionalidade e pela constante mutação tecnológica.

O segundo objetivo específico consistiu em analisar as propostas legislativas e doutrinárias recentes voltadas à construção de novos tipos penais para os crimes cibernéticos, com destaque para os limites constitucionais impostos pelo princípio da legalidade. A pesquisa evidenciou que há um movimento crescente de atualização normativa, tanto no plano nacional quanto internacional, impulsionado pela necessidade de enfrentar práticas como fraudes digitais, ransomware, ataques a sistemas e crimes em ambientes virtuais imersivos. Todavia, também se verificou o risco de um expansionismo penal simbólico, caracterizado pela criação de tipos abertos ou excessivamente genéricos, capazes de comprometer a taxatividade e a previsibilidade da norma penal. Desse modo, o estudo reforça que qualquer inovação legislativa deve ser conduzida com rigor técnico, respeitando os limites constitucionais da legalidade, da proporcionalidade e da intervenção mínima.

O terceiro objetivo específico buscou avaliar criticamente a necessidade de um novo marco legal penal direcionado à regulamentação das condutas ilícitas em ambientes digitais, considerando aspectos como territorialidade, soberania jurídica e cooperação internacional. A partir da análise do Marco Civil da Internet, da Lei Geral de Proteção de Dados e da Convenção de Budapeste, constatou-se que o enfrentamento dos crimes cibernéticos exige uma abordagem normativa integrada, que vá além do direito penal estrito. A cooperação internacional mostrou-se elemento indispensável, uma vez que a criminalidade digital ultrapassa fronteiras físicas e desafia os critérios clássicos de jurisdição. Nesse sentido, a pesquisa aponta que a construção de um direito penal digital efetivo depende da harmonização entre legislações nacionais e tratados internacionais, sem que isso implique relativização das garantias constitucionais.

O quarto objetivo específico consistiu em investigar de que modo as técnicas de investigação e os instrumentos de cooperação internacional podem ser compatibilizados com as garantias constitucionais da legalidade e da segurança jurídica na persecução penal dos crimes cibernéticos. A análise demonstrou que mecanismos como a preservação de registros, a cadeia de custódia da prova digital, as interceptações telemáticas e a colaboração entre autoridades e provedores são fundamentais para a eficácia investigativa. Contudo, também se evidenciou que tais instrumentos devem ser utilizados de forma estritamente legal, sob controle judicial e com observância ao devido processo legal, sob pena de invalidação das provas e violação de direitos fundamentais. Assim, a efetividade da persecução penal digital está

diretamente condicionada ao equilíbrio entre eficiência investigativa e respeito às garantias constitucionais.

A partir do percurso analítico desenvolvido, foi possível responder ao problema de pesquisa proposto, no sentido de que o princípio constitucional da legalidade permanece como fundamento indispensável para a validade e a legitimidade da tipificação penal no ambiente digital, ainda que enfrente fortes tensões diante da inovação tecnológica. O estudo demonstrou que o Direito Penal brasileiro, em sua configuração atual, não está plenamente estruturado para responder de forma segura e eficaz a todas as modalidades de crimes cibernéticos, sobretudo aquelas marcadas pela sofisticação técnica e pela transnacionalidade. Entretanto, também se constatou que a superação dessas limitações não pode ocorrer por meio de flexibilizações indevidas da legalidade, mas sim por meio de atualização normativa criteriosa, cooperação internacional e fortalecimento dos instrumentos técnico-jurídicos de investigação.

A reserva legal, a anterioridade e a taxatividade permanecem como eixos estruturantes mesmo diante de tecnologias disruptivas. A reconstrução dos critérios de subsunção — núcleo da conduta, bem jurídico, resultado e meios/servidores — mostrou-se adequada para enquadrar práticas digitais com impacto real. Com isso, evitou-se a analogia desfavorável ao acusado e preservou-se a previsibilidade das decisões, requisito indispensável ao Estado de Direito. Quanto à capacidade dos tipos penais tradicionais, verificou-se que diversos delitos conservam aplicabilidade em contextos virtuais, sobretudo quando o resultado lesivo é concreto no plano patrimonial, reputacional ou psíquico. Ao mesmo tempo, emergiram zonas de dúvida relacionadas a coerções sexuais exclusivamente virtuais, manipulações identitárias de avatares e lesões a ativos digitais com valor econômico. Esses pontos recomendam ajustes legislativos parcimoniosos e diretrizes interpretativas para fechar lacunas, sem ampliar desnecessariamente o catálogo penal.

No plano da jurisdição e da competência, ficou evidenciado que os critérios de ação e resultado continuam úteis, mas requerem operacionalização compatível com a pulverização de agentes, vítimas e infraestruturas. A proposta de uma árvore decisória contribui para reduzir conflitos de foro, orientar a definição de conexão e continência e favorecer a cooperação entre autoridades. Em um ambiente transnacional por natureza, essa engenharia procedimental torna-se condição de eficácia. No eixo probatório, consolidou-se a necessidade de protocolos padronizados de cadeia de custódia digital. A correlação entre avatar e pessoa, a preservação de logs e metadados, a aferição de integridade por meio de funções de hash e o registro temporal formam um checklist mínimo para dar confiabilidade à prova. A adoção de formatos de requisição claros e repetíveis às plataformas aumenta a chance de admissibilidade, sem abrir

mão da proteção à privacidade e ao devido processo.

No campo de política criminal, a análise sustentou respostas calibradas à gravidade e materialidade dos danos. Em hipóteses sem contato físico, sanções patrimoniais, restrições de acesso e medidas educativas podem ser suficientes e proporcionais, desde que fundamentadas em necessidade e adequação. O trabalho também propôs guarda-corpos contra a sobrecriminalização, priorizando instrumentos civis, administrativos e de autorregulação sempre que o desvalor da ação e do resultado não justificar a intervenção penal. A investigação reconheceu limitações decorrentes da rapidez tecnológica e da escassez de decisões consolidadas. A efetividade das soluções depende de padrões técnicos compartilhados e da cooperação público-privada em escala nacional e transnacional.

Por isso, recomendou-se a atualização periódica dos instrumentos propostos e a continuidade de pesquisas sobre inteligência artificial generativa, dispositivos hápticos, interoperabilidade e governança de plataformas. Do ponto de vista prático, a principal contribuição consistiu na entrega de ferramentas operacionais: uma matriz de tipicidade para condutas digitais, uma árvore de competência para ambientes descentralizados e um checklist probatório voltado à integridade e atribuição. Esses artefatos reduzem incertezas, orientam a atuação de investigação, acusação e defesa, e fornecem previsibilidade decisória ao Judiciário e às próprias plataformas. Sua aplicação tende a aumentar a eficiência sem sacrificar garantias.

De forma conclusiva, esta dissertação contribui para o debate acadêmico ao evidenciar que o enfrentamento dos crimes cibernéticos exige um Direito Penal tecnicamente atualizado, constitucionalmente comprometido e integrado a políticas públicas de governança digital e segurança da informação. Os resultados apontam que a proteção dos bens jurídicos no ciberespaço não se alcança por meio do alargamento indiscriminado da tipicidade penal, mas pela construção de normas claras, precisas e proporcionais, aliadas à educação digital, à cooperação internacional e ao fortalecimento institucional. Assim, reafirma-se que o princípio da legalidade não constitui um obstáculo à repressão dos crimes digitais, mas, ao contrário, representa a principal garantia de que a resposta penal à criminalidade cibernética seja legítima, eficaz e compatível com os valores do Estado Democrático de Direito.

8 Bibliografia

ALEXANDRIA, JCS de. Gestão de Segurança da Informação–uma proposta para potencializar a efetividade da Segurança da Informação em ambiente de pesquisa científica. Instituto de Pesquisas Energéticas e Nucleares, Universidade de São Paulo, São Paulo, 2009.

ALVES, Bruno Moraes et al. Análise da responsabilização criminal dos criadores e propagadores de "deep fakes" no ordenamento jurídico brasileiro. Caderno Pedagógico, v. 21, n. 6, p. e4348-e4348, 2024.

ARAÚJO, Victor Melo. Segurança Da Informação. Clube de Autores, 2015.

BARBOSA, Luana Cristhine Oliveira; CEZAR, André Althmann; CARVALHO, Thomaz Jefferson. A evolução do direito penal frente às novas tecnologias e o crime de estupro virtual. *Anais Eletrônico* ISBN 978-65-5615-164-9 X Mostra Interna de Trabalhos de Iniciação Científica III Mostra Interna de Trabalhos de Iniciação em Desenvolvimento Tecnológico e Inovação. 2024.

BARROSO, Luís Roberto. *Curso de direito constitucional contemporâneo: os conceitos fundamentais e a construção do novo modelo*. 7. ed. São Paulo: Saraiva Educação, 2018. ISBN 9788547230869

BERLANDA, Rodrigo Grando. Guia de segurança da informação para a conectividade de dispositivos IoT. 2021.

BOTELHO, Daniela Garcia et al. 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.

BRASIL. *Código de Processo Penal* (arts. 158-A a 158-F, cadeia de custódia). Brasília: Presidência da República.

BRASIL. LEI N°12.735, de 30 de novembro de 2012. Brasília: Diário Oficial da União, 2012.

BRASIL. LEI N°12.737, de 30 de novembro de 2012. Brasília: Diário Oficial da União, 2012.

BRASIL. *Lei nº 9.296, de 24 de julho de 1996*. Dispõe sobre interceptações telefônicas e telemáticas. Brasília: Presidência da República.

BRASIL. *Marco Civil da Internet* (Lei nº 12.965, de 23 de abril de 2014). Brasília: Presidência da República.

BRITO, Auriney. *Direito penal informático.* Saraiva Educação SA, 2017.

CHAIKLIN, Harris. Ghost in the Wires. My Adventures as the World's Most Wanted Hacker. 2012.

COLAÇO, Hian Silva. Liability of internet service providers: dialogue between the jurisprudence and the civil mark of internet. Revista dos Tribunais, v. 2017, p. 02-16, 2017.

CONSELHO DA EUROPA. *Convenção de Budapeste sobre Crimes Cibernéticos (CETS 185) – Relatório Explicativo*. Estrasburgo: Council of Europe, 2001.

CONSELHO DA EUROPA. *Protocolo Adicional à Convenção de Budapeste (CETS 189) – Relatório Explicativo*. Estrasburgo: Council of Europe, 2003.

COSTA, Bruno de Lucca Rodrigues. Crimes virtuais: uma análise da falta de tipificação legal dos crimes cibernéticos. *Monografia Jurídica apresentada à disciplina Trabalho de Curso II, da Escola de Direito e Relações Internacionais, Curso de Direito, da Pontifícia Universidade Católica de Goiás (PUCGOIÁS).* 2021.

COSTA, Fernando José da. Locus delicti nos crimes informáticos. 2011. Tese de Doutorado. Universidade de São Paulo.

COSTA, Luís Gustavo Silva; CRUZ, Sarah Aparecida da. A engenharia social e os desafios da segurança da informação nas empresas. In: II Congresso Internacional do Grupo Unis. Fundação de Ensino e Pesquisa do Sul de Minas, 2016.

CUNHA, Vinícius Ferreira; CORTIZO, Vitor Martins. CRIMES CIBERNÉTICOS: Implicações Legais, eficácia das leis existentes e necessidade de adaptação do sistema legal a era digital. Revista Acadêmica Online, v. 10, n. 51, p. 1-18, 2024.

DIAS, Júlia Gabrielly Freitas; DANTAS FILHO, Jerônimo Vieira. Cibercriminalidade: Os crimes cibernéticos e os limites da liberdade de expressão na internet. NATIVA-Revista de

Ciências, Tecnologia e Inovação (ISSN: 2764-1295), v. 8, n. 2, p. 73-82, 2025.

DORIGON, Tais Ross. Crimes digitais: o crime de estupro virtual e sua interpretação à luz do princípio da legalidade. 2024.

FONSECA, Kelly Gonçalves et al. Estupro virtual e sua possível tipificação no código penal. *Libertas Direito,* v. 1, n. 2, 2020.

FRAGA, Bruno; VANGLLER, Thompson. *Técnicas de invasão*. Compilado a partir de videoaulas e pesquisas por Thompson Vangller; idealização do projeto por Bruno Fraga. Londres, 2017. 548 p

FRUMI, Patrícia. Marco Civil da Internet, provedores de informação e responsabilidade civil por cyberbullying. Revista dos Tribunais, v. 1044, p. 145-167, 2022.

GABRIEL, Anderson De Paiva. O pragmatismo como paradigma do Direito Processual Penal contemporâneo. Tecnologia, consenso e whistleblowing. Londrina: Thoth Editora, 2022.

GOMES, Inês. Crimes contra a humanidade e ciberespaço. De Legibus-Revista de Direito da Universidade Lusófona Lisboa, n. 5e6, p. 65-100, 2023.

GOMES, Luis Gustavo Cruz. Princípio da legalidade penal e jogos online. 2024.

GUERRA, Mayelli; CANDEIA, Sarajane Rodrigues. A aplicação do crime de "estupro virtual" frente ao ordenamento jurídico brasileiro: análise segundo o princípio da legalidade. A revisão linguística é de responsabilidade dos autores., 2022.

HERNANDEZ, Erika Fernanda Tangerino; DE TOLEDO, Nathália Karina Abucci. Crimes cibernéticos: seus efeitos revolucionários diante de uma legislação em constante evolução. *Revista Jurídica da UniFil,* v. 17, n. 17, p. 72-84, 2021.

IRIBURE JÚNIOR, Hamilton da Cunha; MARTINS, José Renato; SILVA, Douglas de Morais (Coords.). Direitos fundamentais: multiculturalismo e tecnologia na sociedade globalizada. São Paulo: Saraiva, 2018.

LEONARDI, Marcel. Responsabilidade civil dos provedores de serviços de internet. Editora Juarez de Oliveira, 2005.

LÓSSIO, Claudio Joel Brito. O Direito e o ciberespaço. São Paulo: Editora JusPodivm, 2022.

MAIA, Karolline Barbosa; COSTA, Cezar Henrique Ferreira. CRIMES CIBERNÉTICOS. Revista Ibero-Americana de Humanidades, Ciências e Educação, v. 9, n. 10, p. 109-126, 2023.

MARODIN, Tayla Schuster. *O crime de estupro virtual:(des) necessidade de tipificação pelo ordenamento jurídico brasileiro.* 2021. Dissertação de Mestrado. Pontifícia Universidade Católica do Rio Grande do Sul.

MERLONE, Nicholas Maciel. Breve introdução ao direito penal e criminologia crítica econômica e digital: uma nova abordagem. Revista OWL (OWL Journal)-REVISTA INTERDISCIPLINAR DE ENSINO E EDUCAÇÃO, v. 3, n. 3, p. 1-39, 2025.

MITNICK, Kevin D.; SIMON, William L. *A arte do engano: controlando o elemento humano da segurança.* John Wiley & Sons, 2003.

MONTEL, Izadora Fonseca; DE PAIVA, Jaqueline de Kassia Ribeiro. CRIMES CIBERNÉTICOS: PANORAMA LEGISLATIVO. Revista Ibero-Americana de Humanidades, Ciências e Educação, v. 10, n. 11, p. 4495-4523, 2024.

MOTA, Carlos Henrique De Espindola. Cyberstalking: a necessidade de tipificação no direito penal brasileiro. *Portal de Trabalhos Acadêmicos,* v. 12, n. 1, 2020.

OLIVEIRA, Mozart Gustavo Faria de. Repensando os tipos penais do crime permanente, crime instantâneo de efeito permanente e do crime continuado no âmbito da rede mundial de computadores e redes sociais. Qual a melhor forma de qualificação do stalking agora previsto no Art. 147 A do Código Penal Brasileiro? 2023. 71 f. Trabalho de Conclusão de Curso (Bacharelado em Direito) - Faculdade Nacional de Direito, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2023.

PORTELA, Paulo Henrique Gonçalves. Direito internacional público e privado. 2025.

PRESTES, Felipe Pinheiro; ANACLETO, Elvis Preis. JURISDIÇÃO CRIMINAL E DELITOS INFORMÁTICOS: REFLEXOS NA JURISDIÇÃO BRASILEIRA DA CONVENÇÃO DE BUDAPESTE. Anais do Seminário Internacional em Direitos Humanos e Sociedade, v. 6, 2024.

QUEIROZ, Liv Ferreira Augusto Severo. Os crimes cibernéticos no ordenamento jurídico brasileiro: investigação criminal e desafios. Revista do CNMP, n. 12, p. 417-448, 2024.

SANTANA, Gabriel Côvolo. Crimes cibernéticos: necessidade do aprimoramento da tipificação penal dos crimes cibernéticos. *Artigo Científico apresentado à disciplina Trabalho de Curso II, da Escola de Direito, Negócios e Comunicação, Curso de Direito, da Pontifícia Universidade Católica de Goiás (PUCGOIÁS).* 2021.

SANTIAGO, Anna Beatriz Vilhena; PICANÇO, Sarah Ruth Gondim; DIAS, Jean Carlos. A responsabilidade civil na ocorrência de exposição de crianças e adolescentes na internet. Revista Jurídica do Cesupa, v. 5, n. 1, p. 10-32, 2024.

SILVA, Amanda Scalisse. JURISDIÇÃO PENAL NA ERA DIGITAL: TERRITORIALIDADE E DELIMITAÇÃO JURISDICIONAL NO CIBERESPAÇO. In: Congresso Internacional de Direitos Humanos de Coimbra. 2024.

SILVA, Fernanda Bílio et al. A tipificação das condutas praticadas em ambiente virtual. *NOVOS DIREITOS,* v. 10, n. 1, p. 74-88, 2023.

SILVA, Maicon Herverton Lino Ferreira; COSTA, Veridiana Alves de Sousa Ferreira; PERNAMBUCO, Unidade Acadêmica de Serra Talhada. O fator humano como pilar da Segurança da Informação: uma proposta alternativa. v. 23, p. 4, 2023.

SILVA, Maria Gabriella Lira Barboza. Crime cibernético: o crime de estupro virtual e a ausência do contato físico para tipificação. *Portal de Trabalhos Acadêmicos*, v. 13, n. 2, 2021.

SIQUEIRA, Kelly Cristyne Rodrigues. A tipificação do crime de estupro virtual no código penal brasileiro. *Novos Direitos* v.10, n.1, jan.- jun. 2023, p.74 - 88 ISSN: 2447 – 1631. 2024.

SOBRINHA, Ana Amélia Fernandes Albuquerque; MESSIAS, Marcos Venicius Nunes; TEMPONI, Pedro Henrique Araujo. RESPONSABILIZAÇÃO PENAL NOS CRIMES CIBERNÉTICOS: UM ESTUDO SOBRE A LEGISLAÇÃO BRASILEIRA E A SEGURANÇA JURÍDICA. Estudos de Direito Penal e Processo Penal na Contemporaneidade: 2a Edição, 2025.

SOUZA, Luiza Ananda Queiroz; CERVINSKI, Yasmin. É POSSÍVEL A PREVENÇÃO E COMBATE AOS TEMIDOS CRIMES VIRTUAIS?. *Anuário Pesquisa e Extensão Unoesc São Miguel do Oeste,* v. 6, p. e27776-e27776, 2021.

SQUADRI, Ana Carolina. O princípio da aderência da jurisdição ao território na era digital. In: Revista de Processo. 2022. p. 473-483.

TAVARES, Juarez. Projeto de Código Penal: a reforma da parte geral. *Revista da EMERJ,* v. 15, n. 60, p. 161-189, 2012.

TEIXEIRA, André Álisson Leal. Jurisdição e internet: uma releitura da aplicação da lei processual penal no espaço à luz da escala mundial da internet. 2024. Tese de Doutorado. Universidade de São Paulo.

VANDEREI, Matheus Luiz. Políticas públicas para combater crimes virtuais: insuficiência da Lei Geral de Proteção de Dados e adaptações necessárias à regulamentação setorial. Trabalho de Conclusão de Curso (Bacharelado em Direito)-Faculdade Nacional de Direito, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2024.

VICENTE, Gabriel de Andrade. A tipificação do crime de ransomware no direito penal brasileiro. 2022. 31 f. Monografia (Graduação em Direito) - Escola de Direito, Turismo e Museologia, Universidade Federal de Ouro Preto, Ouro Preto, 2022.

WERMUTH, M. A. D.; CALLEGARI, André Luís. Stalking e cyberstalking: considerações críticas sobre o delito tipificado no art. 147-a do Código Penal brasileiro. Revista Brasileira de Ciências Criminais, v. 186, n. 2021, p. 105-126, 2021.