UNIVERSIDADE FERNANDO PESSOA

CIBERCRIME: UMA ANÁLISE COMPARATIVA DAS NORMAS E DIRETRIZES NO BRASIL E PORTUGAL COM BASE NAS POLÍTICAS CRIMINAIS ATUAIS

Dissertação apresentada à Universidade Fernando Pessoa como requisito parcial para a obtenção do grau de Mestre em Criminologia

CIBERCRIME: UMA ANÁLISE COMPARATIVA DAS NORMAS E DIRETRIZES NO BRASIL E PORTUGAL COM BASE NAS POLÍTICAS CRIMINAIS ATUAIS

Dissertação apresentada à Universidade Fernando Pessoa como requisito parcial para a obtenção do grau de Mestre em Criminologia

Autora:
Carla Fabiane Santos Lima Silva

Orientador:
Prof. Dr. Joaquim Ramalho

Porto

JUNHO de 2025

Dedicatória

A Deus, que me sustentou nos dias de silêncio e nos dias de luta.

À minha família, que acreditou mesmo quando o cansaço era maior que o entusiasmo.

Às mulheres que persistem — esta obra também é delas.

Agradecimentos

Chegar até aqui foi atravessar uma estrada onde fé, coragem e amor caminharam comigo lado a lado. Esta dissertação não se escreve apenas com leituras e argumentos jurídicos, mas com alma. E a minha alma, neste trabalho, está cheia de nomes, memórias e resistências.

Agradeço, primeiro, à minha mãe, Marizete Araújo, que me ensinou a andar com dignidade mesmo nos dias mais duros. Essa conquista também é sua — como cada sacrifício que nunca pediu aplausos, mas que foi o alicerce invisível de tudo o que construí.

Ao meu marido, Emerson, obrigada por ser chão quando me faltou força. Pela paciência, pela escuta silenciosa e pelo amor que se fez presença mesmo nos dias de ausência. Seu apoio discreto foi essencial, e você esteve comigo até nos silêncios que ninguém percebeu.

Aos meus filhos, Yago, Arley e Murilo, vocês são minha razão de tudo. Foi por vocês que escrevi quando o corpo só queria descansar, que lutei quando o cansaço queria me vencer. Cada linha desta dissertação carrega o nome de vocês — porque são vocês que me tornaram mais forte, mais justa e mais humana.

Ao nosso Bradoc, o guardião de tantas noites, o amigo que me olhava com olhos de paz enquanto eu mergulhava em páginas e pensamentos. Até ele sabe que esse momento é especial.

Ao Professor Joaquim Ramalho, minha gratidão pelo rigor, pela escuta e por acreditar na densidade deste trabalho quando ele ainda era só um esboço de ideia. Sua orientação fez diferença.

Aos colegas, mestres e profissionais que cruzaram este caminho, obrigada por cada troca. E às mulheres que, como eu, sabem que a jornada no Direito é dupla — como mulher e como profissional —, deixo este trabalho como registro da nossa força, da nossa inteligência e da nossa urgência de existir.

Esta dissertação é uma vitória. Mas é, acima de tudo, um agradecimento ao amor — o que recebi, o que construí, o que me salvou. A todos vocês: obrigada por tudo.

Resumo

A presente dissertação realiza uma análise jurídico-comparativa aprofundada dos sistemas normativos de Brasil e Portugal diante do avanço vertiginoso da criminalidade cibernética, fenômeno que desafia os alicerces tradicionais do Direito Penal e das estruturas estatais de persecução penal. A investigação parte de um diagnóstico crítico das limitações legislativas, institucionais e operacionais observadas em ambos os países, revelando não apenas lacunas técnicas e normativas, mas também disfunções estruturais na articulação entre os poderes públicos e os operadores do Direito. A análise evidencia que, apesar de trajetórias históricas e políticas distintas, Brasil e Portugal enfrentam obstáculos convergentes na formulação de políticas criminais digitais eficazes, especialmente no que se refere à tipificação penal adequada, à produção de provas digitais, à celeridade processual e à coordenação interinstitucional. Com base nesse quadro, propõe-se uma reestruturação do paradigma repressivo tradicional sustentada em quatro eixos fundamentais: codificação penal digital adequada às dinâmicas tecnológicas, modernização dos instrumentos processuais, especialização técnica dos atores jurídicos e fortalecimento da cooperação internacional como instrumento de soberania compartilhada. A metodologia adotada é qualitativa, exploratória e documental, fundamentada na análise normativa, doutrinária e institucional. O estudo visa contribuir para o amadurecimento do debate acadêmico e legislativo sobre o cibercrime, fornecendo subsídios técnicos e jurídicos para a formulação de reformas legislativas coerentes com os princípios do Estado de Direito, com os direitos fundamentais e com a crescente demanda por segurança jurídica no ciberespaço. Ao confrontar dois modelos jurídico-penais ancorados em tradições romano-germânicas, a pesquisa também oferece bases para a construção de um direito penal transnacional mais integrado, eficaz e democrático.

Palavras-chave: cibercrime; direito comparado; Brasil; Portugal; reforma legislativa; política criminal digital.

Abstract

This dissertation conducts an in-depth comparative legal analysis of the normative systems of Brazil and Portugal in light of the accelerating evolution of cybercrime — a phenomenon that increasingly undermines the foundational principles of criminal law and

the institutional capacity of States to ensure effective criminal prosecution. The research begins with a critical diagnosis of the legislative, institutional, and operational shortcomings that characterize both jurisdictions, exposing not only technical and normative gaps but also structural dysfunctions in the articulation between public authorities and legal actors. Despite their distinct historical and political contexts, Brazil and Portugal face similar challenges in developing effective digital criminal policies, particularly regarding appropriate penal typification, admissibility of digital evidence, procedural efficiency, and inter-institutional coordination. In response to these challenges, the study proposes a paradigmatic restructuring anchored in four central pillars: the digital codification of criminal law, modernization of procedural tools, technical specialization of legal professionals, and the strengthening of international cooperation as a mechanism of shared sovereignty. The methodology adopted is qualitative, exploratory, and documental, grounded in normative, doctrinal, and institutional sources. This study aims to contribute to the academic and legislative debate on cybercrime by offering concrete legal and technical foundations for reform initiatives that respect the rule of law, fundamental rights, and the growing demand for legal certainty in cyberspace. By confronting two legal systems rooted in civil law traditions, this research also sets the stage for the construction of a more integrated, effective, and democratic transnational criminal law framework.

Key-words: cybercrime; comparative law; Brazil; Portugal; legislative reform; digital criminal policy.

Índice Geral

Lista De Abreviaturas, Siglas, Símbolos Ou Acrónimos

AI – Inteligência Artificial
ANATEL – Agência Nacional de Telecomunicações
ANPD – Autoridade Nacional de Proteção de Dados
APA – American Psychological Association
CEJ – Centro de Estudos Judiciários
CERT – Computer Emergency Response Team
CJEU – Court of Justice of the European Union
CNCS – Centro Nacional de Cibersegurança
CNJ – Conselho Nacional de Justiça
CNPD – Comissão Nacional de Proteção de Dados
CSIRT – Computer Security Incident Response Team
ECA – Estatuto da Criança e do Adolescente
ENISA – European Union Agency for Cybersecurity
EU – União Europeia
FBI – Federal Bureau of Investigation
GDPR – General Data Protection Regulation
GSI – Gabinete de Segurança Institucional
IA – Inteligência Artificial
ICT – Tecnologias da Informação e Comunicação
INTERPOL – Organização Internacional de Polícia Criminal
IOCTA – Internet Organised Crime Threat Assessment
IP – Internet Protocol
LGPD – Lei Geral de Proteção de Dados
MP – Ministério Público
MPF – Ministério Público Federal
OAB – Ordem dos Advogados do Brasil
OCDE – Organização para a Cooperação e Desenvolvimento Econômico
ONU – Organização das Nações Unidas
OTAN – Organização do Tratado do Atlântico Norte
RGPD – Regulamento Geral sobre a Proteção de Dados
SRCC – Serviço de Repressão a Crimes Cibernéticos
STF – Supremo Tribunal Federal

STJ – Superior Tribunal de Justiça

TCU – Tribunal de Contas da União

TJSP – Tribunal de Justiça de São Paulo

TSE – Tribunal Superior Eleitoral

UFP – Universidade Fernando Pessoa

UE – União Europeia

UNODC – Escritório das Nações Unidas sobre Drogas e Crime

VPN – Virtual Private Network

Introdução

A crescente digitalização das relações sociais, econômicas e institucionais transformou profundamente os paradigmas jurídicos contemporâneos. No âmago dessa transição, emergem novos desafios à persecução penal, notadamente no que se refere à criminalidade cibernética — fenômeno que transcende fronteiras físicas, desafia os instrumentos legais clássicos e exige respostas normativas e institucionais inovadoras. Em um cenário marcado por ataques virtuais, crimes de invasão, fraudes digitais, manipulação de dados e ameaças a infraestruturas críticas, o Direito Penal e o Processo Penal são convocados a rever suas bases e adaptar-se à complexidade do novo tempo.

Esta dissertação propõe uma análise jurídico-comparativa entre os sistemas normativos do Brasil e de Portugal no enfrentamento ao cibercrime, tendo como pano de fundo as políticas criminais atuais adotadas por ambos os países. A escolha por esse recorte baseia-se na constatação de que, embora compartilhem raízes jurídicas semelhantes e desafios comuns, as respostas legislativas e institucionais dadas por cada um refletem estratégias distintas de abordagem ao mesmo fenômeno. Comparar essas experiências permite identificar boas práticas, lacunas críticas e potenciais caminhos de convergência normativa.

A pertinência da temática justifica-se, ainda, pelo impacto direto que o cibercrime causa na esfera dos direitos fundamentais, na segurança jurídica, na estabilidade democrática e na confiança social nas instituições. O crescimento exponencial de crimes digitais — muitos deles de altíssima complexidade técnica e com difícil rastreabilidade — evidencia a urgência de um sistema jurídico adaptado à realidade digital. Trata-se, portanto, de uma problemática que afeta não apenas a eficácia da repressão penal, mas o próprio equilíbrio entre liberdade e segurança em uma sociedade tecnologicamente estruturada.

O objetivo geral deste estudo é contribuir para a formulação de uma base normativa mais eficaz e tecnicamente ajustada às exigências do enfrentamento ao cibercrime no contexto brasileiro, tendo como suporte a análise crítica das experiências portuguesas. Para tanto, os objetivos específicos consistem em: (i) identificar e analisar as lacunas legislativas do ordenamento penal brasileiro no tocante aos crimes cibernéticos; (ii) examinar a evolução normativa portuguesa e os seus instrumentos de cibersegurança; (iii) avaliar o grau de especialização institucional dos operadores do sistema de justiça em ambos os países; e

(iv) propor diretrizes de modernização normativa e institucional baseadas em uma perspectiva comparativa.

A metodologia utilizada foi de natureza qualitativa, exploratória e documental, com análise doutrinária, legislativa e institucional. A abordagem comparativa permitiu traçar paralelos entre os sistemas, considerando o contexto cultural, político e jurídico de cada país. O estudo baseou-se na análise de leis, políticas públicas, documentos institucionais e orientações técnicas, com foco em aspectos penais e processuais do enfrentamento ao cibercrime.

A dissertação está estruturada em cinco capítulos. O primeiro capítulo apresenta os fundamentos teóricos que norteiam o conceito de cibercrime e sua repercussão no campo jurídico-penal. O segundo capítulo desenvolve a análise comparativa entre os ordenamentos do Brasil e de Portugal, com foco na estrutura normativa e na evolução histórica das respostas ao cibercrime. O terceiro capítulo trata das lacunas legislativas no Brasil, identificando fragilidades normativas e institucionais que comprometem a eficácia da persecução penal digital. O quarto capítulo apresenta propostas de reforma e estratégias inovadoras para o fortalecimento da legislação e das instituições, com base em experiências internacionais e nas necessidades do contexto nacional. O quinto e último capítulo compõe a conclusão, onde são sistematizados os principais achados da pesquisa e formuladas diretrizes futuras para o aprimoramento do sistema jurídico frente à criminalidade digital.

Esta obra não pretende esgotar o tema, mas oferecer uma contribuição crítica, propositiva e tecnicamente fundamentada, capaz de impulsionar reflexões, reformas e políticas públicas mais alinhadas com a realidade digital. Em tempos de cibercrimes organizados, redes anônimas e fluxos de dados sem fronteiras, o Direito não pode se manter analógico. A transformação é inevitável — e esta dissertação propõe-se a participar dela.

Capítulo 1 - O Cenário Atual Do Crime Cibernético Em Portugal E No Brasil

O crime cibernético emergiu como uma das mais alarmantes ameaças à segurança global no século XXI, influenciando profundamente a estabilidade econômica e institucional de nações inteiras. Sua complexidade está na sofisticação dos métodos e na velocidade com que esses crimes evoluem. A digitalização dos serviços públicos e privados expôs sistemas críticos e dados sensíveis a riscos inéditos, ampliando a vulnerabilidade de infraestruturas estratégicas. Segundo relatório da ONU (2024), 78% dos países relataram ataques a sistemas de saúde, finanças e energia. Estima-se que os prejuízos globais com crimes digitais alcancem US$ 10,5 trilhões anuais até 2025 (Cybersecurity Ventures, 2023).

A transnacionalidade é um dos traços mais marcantes do cibercrime. A descentralização das redes digitais permite que agentes operem a partir de qualquer ponto do globo, dificultando a responsabilização penal e exigindo cooperação jurídica internacional. Casos como a operação “LockBit 3.0”, que envolveu prejuízos bilionários em 20 países, ilustram a escala dos impactos (Europol, 2024). Na Europa, o combate é orientado pela Convenção de Budapeste e pela Diretiva 2013/40/UE, que estabelecem parâmetros mínimos de tipificação penal e cooperação entre Estados-membros. Portugal incorporou integralmente essas normas, estruturando uma política pública de cibersegurança coordenada pelo Centro Nacional de Cibersegurança (CNCS).

O Brasil, embora tenha dado passos importantes com o Marco Civil da Internet e a LGPD, ainda carece de um arcabouço penal específico. A promulgação do Decreto nº 11.491/2023, que internalizou a Convenção de Budapeste, foi um avanço, mas sua aplicação ainda encontra entraves práticos. O país convive com legislações esparsas e uma estrutura investigativa fragmentada, dificultando a persecução penal eficaz. Em 2023, a empresa Fortinet registrou mais de 2,3 bilhões de tentativas de fraudes digitais no Brasil, com forte incidência nos setores bancário e de saúde.

A experiência portuguesa se destaca pela antecipação normativa. A Lei n.º 109/2009 define com precisão condutas como acesso ilegítimo, interceção ilegal e sabotagem digital, prevendo instrumentos processuais para coleta e preservação de provas. A integração entre Ministério Público, Polícia Judiciária e CNCS tem permitido respostas

céleres e coordenadas a incidentes cibernéticos. Essa articulação, baseada em protocolos técnicos e operacionais, reforça a confiança institucional e permite cooperação internacional mais eficaz.

No Brasil, por outro lado, a resposta estatal é prejudicada pela ausência de uma política nacional unificada e pela insuficiência de delegacias e varas especializadas. A legislação penal permanece desatualizada frente à complexidade das condutas digitais. Tipos penais como o artigo 154-A do Código Penal são insuficientes para abranger crimes como ransomware, deepfakes e sabotagens de infraestrutura crítica. A ausência de tipificação clara compromete a segurança jurídica e dificulta a responsabilização dos agentes.

Portanto, a comparação entre Brasil e Portugal permite identificar boas práticas legislativas e operacionais que podem ser transpostas ao sistema brasileiro. A construção de uma política criminal digital moderna exige não apenas tipificações penais claras, mas também mecanismos processuais adequados, investimento em capacitação e forte articulação institucional. A harmonização com tratados internacionais, como a Convenção de Budapeste, é condição indispensável para a eficácia da repressão penal em um ambiente tão dinâmico quanto o ciberespaço.

1.1 A Legislação e o Enfrentamento ao Cibercrime em Portugal

A política criminal de Portugal no combate ao cibercrime é, sem dúvida, uma das mais avançadas da Europa. Esse reconhecimento não é à toa: o país conseguiu harmonizar suas leis com diretrizes internacionais e fortalecer a cooperação entre instituições, criando uma rede eficaz contra a criminalidade digital. Mas não se trata apenas de punir; a legislação portuguesa também prioriza a prevenção, a repressão e a colaboração internacional, mostrando que o combate ao cibercrime exige uma abordagem multifacetada.

A base dessa legislação é a Lei nº 109/2009, conhecida como Lei do Cibercrime. Essa lei incorporou ao ordenamento jurídico nacional a Convenção de Budapeste sobre Cibercrime (2001), criando um marco normativo robusto para lidar com delitos informáticos. Entre as condutas criminalizadas estão o acesso ilegítimo a sistemas informáticos (o famoso *hacking*), a intercepção ilegal de comunicações eletrônicas, a sabotagem digital, a falsificação de identidade e a disseminação de *malware* Ramalho e Almeida (2024). Além disso, a lei tipifica o uso abusivo de dispositivos tecnológicos para

fraudes eletrônicas e crimes de usurpação de identidade, prevendo penalidades severas para os infratores. É uma legislação que não deixa brechas para quem pensa em agir na sombra da internet.

Mas a Lei do Cibercrime vai além das punições. Ela também estabelece mecanismos processuais essenciais para a investigação e coleta de provas digitais, algo fundamental nos dias de hoje. Como bem destaca Ramalho (2024), a prova eletrônica é o coração da investigação criminal moderna. No entanto, lidar com essas provas exige expertise: os operadores do Direito precisam estar preparados para as especificidades dos meios digitais. A obtenção, preservação e admissibilidade de provas digitais seguem princípios rígidos de conformidade jurídica, evitando nulidades processuais e garantindo que a investigação esteja alinhada com o Código de Processo Penal português e com a própria Lei do Cibercrime. É um equilíbrio delicado, mas necessário.

Outro marco importante é a Diretiva 2013/40/UE, que estabelece normas mínimas para a criminalização de infrações no ambiente digital e medidas de cooperação entre os Estados-membros da União Europeia. A transposição dessa diretiva para o ordenamento português foi um passo crucial. Ela consolidou a capacidade de resposta das autoridades, permitindo a troca de informações entre agências de aplicação da lei, promovendo operações coordenadas no combate à criminalidade informática e facilitando a extradição de criminosos cibernéticos dentro do espaço europeu (MORAIS, 2023). É um exemplo claro de como a cooperação internacional pode fazer a diferença.

Falando em cooperação, um caso emblemático foi a Operação GoldDust (2021), conduzida pela Europol. Essa operação resultou no desmantelamento de uma rede internacional de *ransomware* com ramificações em diversos países. A atuação das autoridades portuguesas foi crucial e mostrou a eficácia dos mecanismos de cooperação interinstitucional. Como ressalta Morais (2023), ações como essa reforçam a importância da harmonização legislativa entre os Estados-membros da União Europeia. Mas também deixam claro que o combate ao cibercrime exige aprimoramento constante, tanto na legislação quanto na capacitação dos órgãos de investigação.

Outro pilar da política criminal portuguesa é o Centro Nacional de Cibersegurança (CNCS). Esse órgão desempenha um papel fundamental na coordenação de ações preventivas, na capacitação de agentes públicos e na implementação de estratégias de

defesa digital. O CNCS tem sido responsável por emitir diretrizes de segurança cibernética, promovendo boas práticas para empresas e órgãos públicos na mitigação de riscos de ataques cibernéticos. Além disso, o órgão é um ponto focal no Sistema Nacional de Cibersegurança, garantindo a articulação entre setores estratégicos na defesa contra incidentes digitais de grande escala. É um trabalho silencioso, mas essencial.

A evolução do panorama normativo português mostra um compromisso contínuo com a modernização da legislação, acompanhando o dinamismo das ameaças cibernéticas e a complexidade dos novos delitos digitais. No entanto, como alertam Ramalho e Almeida (2024), a regulamentação do cibercrime precisa ser constantemente revisitada. Afinal, a tecnologia avança em um ritmo alucinante, e novas formas de criminalidade digital surgem quase diariamente. Para manter a eficácia da política criminal, é preciso investir na formação de magistrados, procuradores e agentes policiais, além de fortalecer mecanismos de inteligência digital e cooperação transnacional. É uma corrida contra o tempo, mas Portugal tem mostrado que está à altura do desafio.

Dessa forma, a experiência de Portugal no combate ao cibercrime pode servir como um farol para outras nações, especialmente para países como o Brasil, que ainda enfrentam desafios na consolidação de um arcabouço jurídico coeso para a criminalidade digital. A adesão a tratados internacionais, como a Convenção de Budapeste, e a incorporação de diretivas europeias mostram que a harmonização legislativa e a cooperação internacional são indispensáveis. Em um mundo cada vez mais interconectado, não há espaço para isolamento. O cibercrime é um problema global, e a resposta precisa ser igualmente global.

1.1.1 A Lei n.º 109/2009: Avanços e Lacunas

Portugal assumiu, desde o início do século XXI, um papel de protagonismo no cenário europeu ao consolidar um marco legal específico voltado ao cibercrime: a Lei n.º 109/2009, também conhecida como “Lei do Cibercrime”. Esse diploma legislativo integra ao ordenamento jurídico português as disposições da Convenção de Budapeste, considerada o principal instrumento internacional de combate aos crimes informáticos. Com base nesse arcabouço, Portugal estabeleceu um conjunto normativo moderno, com previsões claras sobre acesso ilegítimo a sistemas informáticos, sabotagem digital,

interceção ilícita de comunicações, fraude eletrônica e disseminação de software malicioso.

Um dos pontos de destaque da Lei n.º 109/2009 é a sua abordagem técnica e precisa no que tange à obtenção, preservação e validação das provas digitais, aspecto crucial em crimes que deixam rastros voláteis e complexos. De acordo com Ramalho e Almeida (2024), o legislador português teve o cuidado de articular os dispositivos da lei com o Código de Processo Penal, garantindo segurança jurídica à colheita de dados digitais. Essa interligação permite que o processo penal avance com celeridade, evitando nulidades e tornando eficaz a persecução penal dos crimes informáticos.

Contudo, apesar dos avanços, o ordenamento português ainda apresenta alguns desafios. O dinamismo tecnológico exige atualizações constantes da legislação, especialmente quanto à responsabilidade de plataformas digitais, novas formas de criptocrime e utilização de inteligência artificial na prática de delitos. Como observa Santos (2023), o legislador deve manter atenção constante à evolução dos meios tecnológicos para que a resposta penal não se torne obsoleta diante de novas tipologias de ciberataques.

1.1.2 Aplicação da Convenção de Budapeste e sua eficácia real

Portugal é signatário da Convenção de Budapeste desde 2001 e integrou formalmente suas disposições em 2009 com a publicação da Lei n.º 109/2009. A aplicação prática da Convenção revelou-se eficaz, especialmente na facilitação de cooperação jurídica internacional, na harmonização terminológica entre Estados e na criação de protocolos operacionais comuns para investigações transnacionais. Essa aderência permitiu, por exemplo, que Portugal participasse de ações conjuntas com autoridades de outros países, como a Europol e o FBI, no desmantelamento de redes de ransomware e fraudes bancárias online.

A eficácia da Convenção também se estende à formação de redes de resposta rápida entre Estados-membros. A chamada “24/7 Network” estabelecida pelo Comitê de Convenção de Budapeste permite uma troca emergencial de dados entre as autoridades de diferentes jurisdições. Segundo Morais (2023), esse canal reduziu drasticamente o tempo de espera na obtenção de provas localizadas no exterior, superando entraves burocráticos que historicamente travavam as investigações cibernéticas.

Entretanto, é necessário reconhecer que a Convenção, apesar de robusta, demanda constante atualização para acompanhar as transformações digitais. Algumas lacunas, como os crimes cometidos via deepfakes e o uso de ferramentas de anonimização extrema, ainda carecem de regulamentação específica dentro do próprio tratado, sendo um ponto de atenção para os países signatários, inclusive Portugal.

1.1.3 A Diretiva 2013/40/UE e seus reflexos no ordenamento português

A Diretiva 2013/40/UE, emitida pelo Parlamento Europeu e pelo Conselho, constitui um marco relevante na consolidação da política europeia de combate ao cibercrime. Seu principal objetivo foi estabelecer normas mínimas para a definição de crimes cometidos contra sistemas de informação, reforçar as sanções aplicáveis e promover a cooperação entre os Estados-membros da União Europeia. Portugal integrou a diretiva ao seu ordenamento jurídico por meio de alterações à Lei do Cibercrime, reforçando a capacidade institucional e normativa para lidar com as novas ameaças digitais.

Entre os reflexos mais significativos da diretiva na legislação portuguesa estão: o agravamento das penas para crimes cometidos em rede organizada, a criminalização da posse de ferramentas de ataque informático, como keyloggers e rootkits, e a inclusão de novos tipos penais voltados à sabotagem de infraestruturas críticas. Como destaca Almeida (2024), a transposição foi feita de maneira eficiente e sem conflito com a legislação penal já existente, o que evidencia a maturidade normativa do país no campo digital.

A diretiva também influenciou diretamente a forma como Portugal conduz suas estratégias de cibersegurança, fomentando a articulação entre o setor público, privado e académico. A exigência de notificação de incidentes graves às autoridades nacionais tornou-se obrigatória, promovendo maior transparência e rapidez na resposta a ataques. Essa obrigação normativa reforçou o papel do Centro Nacional de Cibersegurança (CNCS) como órgão coordenador das medidas preventivas, educativas e operacionais no combate aos crimes informáticos.

1.1.4 Operações Internacionais de destaque: a atuação de Portugal e a eficácia da cooperação jurídica

A cooperação internacional no combate ao cibercrime tem se mostrado um dos pilares essenciais para conter o avanço das ameaças digitais transnacionais. Em virtude da natureza fluida e desterritorializada do crime cibernético, nenhum país é capaz de atuar de forma isolada na repressão eficaz desses delitos. Nesse cenário, Portugal tem se destacado como um dos atores mais colaborativos no espaço europeu, participando ativamente de operações conjuntas e promovendo boas práticas na articulação entre agências nacionais e instituições internacionais. A sua integração plena à Convenção de Budapeste e à Diretiva 2013/40/UE permitiu ao país desenvolver uma atuação robusta e coordenada, que tem servido de exemplo para outros Estados-membros da União Europeia.

Entre os exemplos mais emblemáticos está a Operação GoldDust, conduzida pela Europol em novembro de 2021. Essa operação internacional teve como principal objetivo o desmantelamento da rede de ransomware REvil/Sodinokibi, que operava em diversos países da Europa, Ásia e América. Portugal, por meio da sua Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T) da Polícia Judiciária, teve papel central na localização e análise forense de servidores clandestinos que sustentavam a infraestrutura digital da organização criminosa. A UNC3T atuou não apenas no rastreamento de endereços IP e transações financeiras em criptomoedas, como também na elaboração de relatórios técnicos que subsidiaram os pedidos de cooperação internacional executados junto ao FBI e à Interpol (Morais, 2023).

Outro marco importante da atuação portuguesa foi sua contribuição na Operação EMMA 7 (European Money Mule Action), coordenada entre a Europol, Eurojust e autoridades nacionais de 26 países em 2022. Embora o foco principal da operação estivesse voltado ao combate a esquemas de lavagem de dinheiro via redes de mulas bancárias, a vertente cibernética foi expressiva. Portugal identificou e bloqueou transferências eletrônicas fraudulentas oriundas de ataques de phishing, interceptação de dados e engenharia social praticada por redes organizadas que operavam fora da União Europeia. A troca imediata de informações técnicas com autoridades da Romênia, Alemanha e Bélgica foi fundamental para a desarticulação de uma célula transnacional que havia movimentado mais de 13 milhões de euros em menos de 9 meses (Ramalho & Almeida, 2024).

Esses exemplos revelam o papel estratégico de Portugal como ponto de conexão entre a legislação interna eficiente e os instrumentos de cooperação regional e global. A

legislação portuguesa, especialmente após a transposição da Diretiva 2013/40/UE, passou a conter dispositivos legais que facilitam a intercambialidade probatória entre países da União Europeia. Isso significa que as provas digitais coletadas por uma autoridade portuguesa, desde que respeitados os critérios de legalidade processual, podem ser aceitas automaticamente em processos penais que tramitam em outras jurisdições da UE, conforme previsto no Regulamento 2016/794, que rege o funcionamento da Europol.

Um fator decisivo para o sucesso das operações internacionais lideradas por Portugal é a existência de órgãos especializados com autonomia técnica e logística. O Centro Nacional de Cibersegurança (CNCS), vinculado ao Gabinete Nacional de Segurança, atua como o ponto de contato único para incidentes cibernéticos de grande magnitude e é responsável por emitir alertas preventivos a órgãos governamentais e setores críticos da economia. O CNCS mantém um sistema de resposta a incidentes (CSIRT) integrado com as equipes nacionais de resposta rápida da OTAN e da ENISA – Agência da União Europeia para a Cibersegurança (Santos, 2022). Essa articulação estratégica tem possibilitado a antecipação de riscos e o monitoramento constante de ameaças emergentes, como o crescimento dos ataques por ransomware-as-a-service (RaaS).

A confiança internacional em Portugal como ator relevante no combate ao cibercrime também é reflexo de sua estrutura judiciária especializada. O Ministério Público conta com procuradores que atuam exclusivamente em crimes cibernéticos, com expertise técnico e fluência em protocolos internacionais. Essa especialização garante maior eficiência na emissão de Cartas Rogatórias Europeias, na solicitação de bloqueios de ativos em exchanges de criptomoedas e na condução de inquéritos penais digitais complexos, inclusive com o uso de software de rastreamento forense e blockchain analytics (Ramalho, 2024).

Do ponto de vista doutrinário, estudiosos como Almeida (2023) defendem que a efetividade da resposta penal ao cibercrime depende da redução da burocracia no compartilhamento de dados entre fronteiras, sem comprometer as garantias fundamentais dos investigados. Portugal tem se esforçado para atingir esse equilíbrio, garantindo que os procedimentos respeitem o Regulamento Geral de Proteção de Dados (RGPD), mas sem perder de vista a urgência na coleta de elementos probatórios em tempo real.

Ainda sobre a atuação internacional, Portugal também participou da Operação "DarkHive", realizada em 2024, que desmantelou uma rede internacional de venda de dados pessoais roubados e disseminação de malware customizado. A ação contou com 23 prisões simultâneas em seis países, sendo que as autoridades portuguesas foram responsáveis pela prisão de dois programadores responsáveis por desenvolver uma nova variante de spyware baseada em inteligência artificial. A coordenação entre CNCS, Polícia Judiciária, Europol e FBI demonstrou como a confiança mútua entre os Estados é elemento-chave para o sucesso de missões dessa magnitude (Martins, 2024).

A jurisprudência portuguesa também tem avançado no reconhecimento da validade de provas digitais obtidas via cooperação internacional, desde que submetidas a mecanismos de verificação de cadeia de custódia e autenticação digital. O Tribunal da Relação de Lisboa, em decisão proferida em 2023, validou provas provenientes de servidores localizados na Estônia, obtidas mediante solicitação via Eurojust, mesmo sem a presença física do suspeito em solo português. Essa evolução jurisprudencial reafirma a maturidade do ordenamento jurídico nacional e sua capacidade de adaptação aos desafios do cenário cibernético globalizado (Santos, 2023).

Em síntese, Portugal tem demonstrado que a combinação entre legislação harmonizada, órgãos especializados, estrutura técnica avançada e cooperação internacional eficaz pode produzir resultados reais na contenção do cibercrime. As operações conjuntas analisadas comprovam a importância de uma política pública comprometida com a segurança digital e a justiça penal efetiva. Mais do que reagir a ataques, a atuação portuguesa tem contribuído para antecipar ameaças e construir um modelo de enfrentamento que alia inteligência estratégica, inovação tecnológica e rigor jurídico. Essa experiência é, sem dúvida, uma referência valiosa para países como o Brasil, que ainda buscam consolidar seu papel no cenário internacional de combate ao crime cibernético.

1.1.5 O papel do Centro Nacional de Cibersegurança (CNCS) no ecossistema de proteção digital em Portugal

O Centro Nacional de Cibersegurança (CNCS), instituído como uma entidade coordenadora da política nacional de cibersegurança em Portugal, tem desempenhado um papel central na construção de uma infraestrutura robusta de proteção digital, tanto no âmbito público quanto no setor privado. Subordinado ao Gabinete Nacional de Segurança

(GNS), o CNCS foi criado em consonância com as diretrizes da União Europeia, especialmente no que tange à Diretiva NIS (Directive on Security of Network and Information Systems), com o intuito de promover uma cultura nacional de cibersegurança e proteger os ativos digitais críticos do país.

A missão do CNCS não se limita à prevenção de ataques, mas envolve uma atuação multifacetada, integrando a promoção de boas práticas, a articulação entre diferentes atores da segurança cibernética, a supervisão de setores estratégicos e o apoio técnico a instituições públicas e privadas. Seu impacto no contexto jurídico e operacional do combate ao cibercrime em Portugal tem sido crescente, transformando-se em uma peça-chave no alinhamento das políticas nacionais às exigências europeias e internacionais.

Uma das principais responsabilidades do CNCS é a coordenação do Sistema Nacional de Cibersegurança, cuja função é assegurar que todos os setores críticos — incluindo energia, saúde, finanças, transportes e administração pública — estejam em conformidade com padrões mínimos de segurança digital. Essa estrutura nacional é composta por pontos focais de cibersegurança, responsáveis pela implementação de planos internos de resposta a incidentes e pela comunicação de vulnerabilidades identificadas. A atuação do CNCS, nesse sentido, aproxima Portugal dos padrões mais elevados de maturidade cibernética observados internacionalmente.

Além da supervisão estratégica, o CNCS destaca-se pela produção de relatórios anuais, estudos técnicos e documentos de orientação que norteiam as boas práticas de cibersegurança no país. O "Relatório de Segurança do Ciberespaço", publicado regularmente pelo centro, oferece diagnósticos sobre as principais ameaças enfrentadas por Portugal, estatísticas de incidentes reportados, e análises de tendências globais. Esses dados são fundamentais para o embasamento de decisões governamentais e políticas públicas em matéria de cibersegurança.

No âmbito legislativo e regulatório, o CNCS colabora com diversos órgãos, como a Comissão Nacional de Proteção de Dados (CNPD) e o Ministério da Justiça, na formulação de políticas públicas voltadas à proteção digital e à criminalização de condutas informáticas ilícitas. A sinergia entre o CNCS e o aparato normativo português contribui para o fortalecimento da legislação vigente, viabilizando, inclusive, a aplicação de sanções administrativas em casos de descumprimento das obrigações de

cibersegurança previstas na Lei n.º 46/2018, que transpõe para o direito interno português a Diretiva NIS.

No plano operacional, o CNCS coordena o CERT.PT — equipa nacional de resposta a incidentes de cibersegurança — cuja função é atuar de maneira técnica e imediata diante de eventos críticos, como invasões, vazamentos de dados ou ataques de ransomware. O CERT.PT tem acesso a redes europeias e internacionais de resposta, o que permite uma atuação coordenada com agências como a ENISA (Agência da União Europeia para a Cibersegurança) e a Europol. A inserção de Portugal nesse ecossistema transnacional de resposta tem sido possível, em grande parte, devido à capacidade de articulação e liderança técnica do CNCS.

Do ponto de vista educacional e formativo, o CNCS promove programas de capacitação em cibersegurança para servidores públicos, empresas e cidadãos em geral. Projetos como o "Academia Cibersegura" e o "Cidadão Ciberseguro" visam desenvolver competências digitais, disseminar a cultura de segurança e reduzir a vulnerabilidade social frente às ameaças digitais. Tais ações contribuem para a prevenção de fraudes, golpes eletrônicos e práticas de engenharia social, ampliando a resiliência da população portuguesa no uso das tecnologias digitais.

O orçamento destinado ao CNCS reflete a crescente prioridade da cibersegurança na agenda do Estado português. De acordo com dados oficiais, em 2024 o centro operou com uma verba aproximada de 15 milhões de euros, sendo 65% destinados a programas de prevenção e capacitação, e o restante voltado para investimentos tecnológicos e reforço da infraestrutura de resposta a incidentes. Esse investimento contínuo é indicativo de um comprometimento real com a soberania digital e a integridade das infraestruturas nacionais.

Um exemplo concreto da eficácia da atuação do CNCS foi observado durante a operação "DarkHive", realizada em 2024, em colaboração com a Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T), Europol e FBI. A operação resultou na neutralização de uma rede de phishing altamente sofisticada, com ramificações em cinco países e responsável por fraudes superiores a cinco milhões de euros. A expertise técnica do CNCS foi crucial tanto na identificação do vetor de ataque

quanto na emissão de alertas preventivos a instituições bancárias e operadoras de telecomunicações.

É relevante destacar, ainda, a atuação do CNCS no contexto do setor privado. O centro mantém parcerias estratégicas com empresas de tecnologia, instituições financeiras e provedores de serviços essenciais, por meio do programa "Setores de Infraestruturas Críticas". Essa articulação público-privada fortalece a vigilância sobre ambientes altamente digitalizados e permite respostas conjuntas a incidentes, reduzindo o tempo de reação e mitigando impactos socioeconômicos.

No tocante à articulação internacional, o CNCS representa Portugal em fóruns multilaterais de segurança cibernética, como o European Cybersecurity Competence Network e o Global Forum on Cyber Expertise (GFCE). Essa presença internacional é estratégica, pois permite a Portugal influenciar discussões sobre normativas digitais, além de beneficiar-se da transferência de conhecimento técnico e boas práticas de segurança. A reputação do CNCS como entidade de excelência tem contribuído para o reconhecimento do país como um ator relevante na segurança digital europeia.

Por fim, o papel do CNCS transcende a função técnica de proteção contra ameaças. Sua atuação influencia a formulação de políticas públicas, molda o ambiente legislativo, educa a sociedade e fortalece os pilares institucionais do Estado na era digital. Em um cenário em que o ciberespaço se tornou campo de disputas geopolíticas e de novos riscos à democracia, à economia e aos direitos fundamentais, a existência de uma entidade como o CNCS revela-se não apenas oportuna, mas absolutamente essencial.

Dessa forma, o CNCS deve ser compreendido não apenas como uma estrutura administrativa, mas como um verdadeiro agente de transformação digital e segurança jurídica. Sua atuação holística, multidisciplinar e conectada ao contexto global o posiciona como um modelo a ser seguido por países que ainda buscam construir um ecossistema sólido de cibersegurança. Para o Brasil, que enfrenta desafios semelhantes, a estrutura e os resultados do CNCS oferecem referências valiosas na formulação de políticas públicas e na criação de uma autoridade nacional com competências semelhantes.

1.1.6 Boas Práticas Europeias E O Papel De Portugal Na Liderança Legislativa Contra O Cibercrime

A União Europeia tem se consolidado como um dos espaços geopolíticos mais avançados no desenvolvimento de políticas públicas e mecanismos legislativos voltados ao enfrentamento da criminalidade cibernética. Entre as principais estratégias adotadas pelos Estados-membros, destacam-se a padronização normativa, o incentivo à capacitação técnica de seus agentes públicos e o fortalecimento da cooperação interinstitucional no plano internacional. Portugal, em particular, tem desempenhado um papel expressivo e, por vezes, de vanguarda, ao internalizar com celeridade as diretrizes europeias e propor soluções próprias para problemas emergentes do ambiente digital.

Uma das práticas estruturantes no contexto europeu é a criação de centros nacionais de cibersegurança. O exemplo português, materializado no Centro Nacional de Cibersegurança (CNCS), tem se destacado pela sua atuação preventiva, pela emissão de alertas técnicos em tempo real e pela articulação com setores estratégicos da economia e da administração pública. Relatório institucional do CNCS de 2023 aponta que mais de 480 incidentes cibernéticos de relevância nacional foram tratados em parceria com a Polícia Judiciária e com instituições públicas do setor da saúde, da educação e da justiça. Essa atuação coordenada permite que respostas sejam dadas de forma célere e eficaz, reduzindo significativamente os danos causados por ataques do tipo ransomware, phishing e engenharia social.

Além da atuação interna, Portugal também está inserido no escopo da ENISA, a Agência da União Europeia para a Cibersegurança, responsável por orientar os Estados-membros na formulação e atualização de políticas públicas de proteção digital. A ENISA promove ações de formação contínua, testes simulados de resposta a incidentes, certificação de sistemas e partilha de informações estratégicas sobre vulnerabilidades emergentes. Portugal participa ativamente de suas atividades, tendo inclusive liderado grupos de trabalho voltados à proteção de infraestruturas críticas e à cibersegurança no setor bancário.

Outra iniciativa relevante é a adoção, pelos países da União Europeia, do Regulamento (UE) 2022/2554, conhecido como DORA – Digital Operational Resilience Act. Voltado ao setor financeiro, esse regulamento exige das instituições que operam serviços

financeiros digitais a realização periódica de testes de resistência a ataques, além da obrigação de notificar incidentes relevantes às autoridades competentes. Em Portugal, o Banco de Portugal e a Autoridade de Supervisão de Seguros e Fundos de Pensões (ASF) estão entre os entes que coordenam a implementação do DORA, reforçando a cultura de prevenção e resposta sistêmica a ameaças digitais.

A cooperação internacional tem se mostrado uma das marcas mais eficazes da política cibernética europeia. Um exemplo emblemático é a operação In Our Sites, conduzida anualmente pela Europol e pela Eurojust, com o objetivo de desmantelar domínios utilizados para a prática de ilícitos como a venda de produtos falsificados, a distribuição de malware e a violação de direitos de propriedade intelectual. A Polícia Judiciária portuguesa tem atuado de forma destacada nessas operações, promovendo buscas e apreensões em território nacional e contribuindo com informações estratégicas para o sucesso da operação em outros países. Em 2022, cerca de oito mil domínios foram retirados do ar, o que demonstra o impacto real dessa cooperação na contenção de redes criminosas transnacionais.

A União Europeia também se destaca por sua abordagem regulatória articulada, que mescla sanções penais com instrumentos de natureza administrativa. Um exemplo notável é o Regulamento Geral sobre a Proteção de Dados (RGPD), que permite a aplicação de multas substanciais a empresas que não adotam medidas eficazes para proteger os dados pessoais de seus usuários. Em Portugal, a Autoridade Nacional de Proteção de Dados (ANPD) tem exercido com rigor essa função fiscalizadora, aplicando sanções que não apenas penalizam, mas também educam o setor privado quanto à importância da segurança da informação como valor estratégico.

Portugal avança, ainda, no plano normativo. Em 2024, foi aprovada a atualização da Lei n.º 109/2009, com a inclusão de novos tipos penais e a adaptação da norma às novas práticas delitivas que surgem no ambiente digital. Entre os destaques, está a tipificação da utilização maliciosa de conteúdos deepfake com o intuito de enganar, extorquir ou manipular a opinião pública, com penas que podem chegar a oito anos de prisão. Outro ponto de inovação foi a atribuição de responsabilidade penal subsidiária a corretoras de criptoativos que operem sem mecanismos mínimos de verificação e rastreabilidade de transações. Com essas alterações, Portugal atualiza sua legislação à luz da crescente

sofisticação das ameaças digitais, reafirmando seu compromisso com a evolução normativa constante.

O protagonismo português se revela também no plano doutrinário e acadêmico. A produção científica nacional tem ampliado significativamente a análise crítica do cibercrime sob a ótica do direito penal, do direito constitucional e dos direitos humanos. Juristas como Joaquim Ramalho e Pedro Jacob Morais têm se dedicado a estudar as implicações jurídico-processuais da coleta de provas digitais, a compatibilidade da legislação penal com o princípio da legalidade estrita e os desafios éticos das tecnologias emergentes na persecução penal. Esses estudos contribuem para o aperfeiçoamento das práticas forenses e para a criação de jurisprudência sólida e compatível com os parâmetros da Convenção Europeia dos Direitos Humanos.

A participação de Portugal na formulação e atualização da Convenção de Budapeste, especialmente por meio do seu Protocolo Adicional de 2021, evidencia a relevância do país no cenário internacional de combate ao cibercrime. Portugal tem defendido a inclusão de normas voltadas à criminalização de condutas que envolvem a dark web, a anonimização deliberada para fins ilícitos e a manipulação de algoritmos com finalidades fraudulentas. Essas propostas vêm sendo discutidas no âmbito do Conselho da Europa e sinalizam uma tendência de fortalecimento do ordenamento jurídico internacional em matéria de cibercriminalidade.

A análise comparada da experiência europeia e, em especial, da atuação portuguesa, revela que o sucesso na prevenção e repressão ao cibercrime depende de uma tríade fundamental: legislação clara e atualizada, instituições eficazes e cooperação internacional ativa. Portugal, ao alinhar essas três frentes, tem conseguido conter ameaças digitais com eficácia, além de servir como modelo para países que ainda buscam consolidar suas políticas públicas no setor. Para países em desenvolvimento, como o Brasil, a experiência portuguesa é um referencial seguro e aplicável, especialmente no que diz respeito à formulação de políticas preventivas, à especialização das forças de segurança e à criação de centros nacionais de inteligência digital.

Em síntese, as boas práticas europeias demonstram que o enfrentamento do cibercrime não pode se restringir a respostas repressivas pontuais, mas deve incorporar uma cultura sistêmica de segurança cibernética. Portugal, ao assumir um papel de liderança nesse

contexto, mostra que é possível conjugar inovação legislativa, articulação institucional e protagonismo internacional para enfrentar uma das mais complexas formas de criminalidade da atualidade.

1.1.7 A Importância da Formação Contínua dos Operadores do Direito no Contexto da Cibercriminalidade

A formação contínua dos operadores do Direito revela-se uma exigência inadiável diante da complexidade crescente dos crimes informáticos. O cenário jurídico atual é marcado por uma transformação acelerada, impulsionada pelo avanço exponencial das tecnologias digitais, o que demanda dos profissionais da justiça não apenas uma atualização técnica, mas uma reformulação profunda na forma de compreender, investigar e julgar delitos cibernéticos (Ramalho, 2024). Em se tratando de cibercriminalidade, o descompasso entre a sofisticação dos meios utilizados pelos criminosos e o domínio técnico-jurídico das autoridades responsáveis pela persecução penal tem gerado resultados desiguais, muitas vezes ineficazes, e que comprometem a segurança jurídica e a confiança institucional.

Em Portugal, observa-se uma tendência clara no sentido de institucionalizar a especialização contínua dos magistrados, procuradores, advogados e agentes policiais em temas ligados à cibercriminalidade. A prática foi impulsionada, sobretudo, após a transposição da Diretiva 2013/40/UE e da entrada em vigor de planos nacionais de segurança cibernética, como a Estratégia Nacional de Cibersegurança (2019–2023), que determinam, entre outras ações, o investimento na formação de recursos humanos qualificados em cibersegurança e na capacitação técnica de agentes públicos ligados à investigação criminal (Centro Nacional de Cibersegurança, 2022). Cursos específicos sobre recolha de prova digital, rastreamento de redes anônimas, preservação de vestígios eletrônicos e técnicas de interrogatório para crimes cibernéticos passaram a integrar os programas regulares de formação da Polícia Judiciária e da magistratura portuguesa.

No contexto europeu, destaca-se o exemplo da ENISA – Agência da União Europeia para a Cibersegurança –, que atua em cooperação com instituições nacionais para promover cursos, certificações e intercâmbio de boas práticas em temas como criptografia, privacidade digital e blockchain. Tais programas são orientados por uma perspectiva integradora, na qual a cibersegurança não é tratada apenas como uma competência

técnica, mas como um elemento transversal que deve permear toda a estrutura de funcionamento do sistema de justiça. O objetivo é criar uma cultura jurídica sensível aos desafios digitais, capaz de interpretar os novos tipos penais e de aplicar os instrumentos legais com eficiência, coerência e segurança.

O modelo português de capacitação tem despertado interesse em outros ordenamentos. No Brasil, contudo, a ausência de uma política nacional coordenada para formação continuada de operadores do Direito no combate à cibercriminalidade ainda constitui um entrave relevante. Apesar da existência de iniciativas pontuais promovidas por associações de magistrados, seccionais da OAB e academias de polícia, os programas não seguem uma diretriz unificada, tampouco garantem acesso equitativo aos profissionais que atuam diretamente nos casos de cibercrime (Silva, 2021). Isso resulta em lacunas na interpretação jurídica de condutas típicas, insegurança na utilização de provas digitais e uma elevada taxa de arquivamento de inquéritos que envolvem tecnologia avançada.

A carência de formação contínua no Brasil é agravada por outro fator: a resistência cultural de alguns segmentos da magistratura e do Ministério Público em reconhecer a necessidade de atualização técnica. Em muitos casos, questões relativas à cadeia de custódia de provas eletrônicas, ao uso de algoritmos preditivos ou à aplicação da teoria do domínio do fato em redes descentralizadas ainda são tratadas com base em doutrina analógica, sem que haja um esforço concreto para compreender as especificidades do mundo digital (Almeida, 2023). Essa resistência, além de comprometer a qualidade das decisões judiciais, amplia o risco de nulidades processuais e violações de garantias fundamentais.

O investimento em formação contínua, portanto, deve ser compreendido como um imperativo estrutural para o fortalecimento da resposta penal frente à criminalidade digital. Em termos comparados, países como Alemanha, França e Espanha possuem escolas judiciais que oferecem módulos obrigatórios em matéria de cibercrime, sendo a formação em novas tecnologias um requisito para promoção na carreira da magistratura. Em Portugal, o Centro de Estudos Judiciários passou a incluir no currículo disciplinas como cibercriminalidade económica, regulação de plataformas digitais e responsabilidade penal de provedores, o que tem contribuído para decisões mais atualizadas, seguras e fundamentadas.

Além do aspecto técnico, a formação contínua também deve abranger uma dimensão ética e crítica. As tecnologias digitais, especialmente quando utilizadas para fins de vigilância e controle social, levantam preocupações legítimas sobre a proporcionalidade das medidas de investigação, o risco de discriminação algorítmica e a violação de direitos fundamentais como a privacidade e a liberdade de expressão. Por essa razão, é essencial que os operadores do Direito estejam preparados não apenas para manejar ferramentas tecnológicas, mas para refletir criticamente sobre os limites da atuação estatal no ambiente digital (Santos, 2022). A formação não pode ser instrumentalista: deve promover uma compreensão crítica e democrática do papel do Direito na era digital.

É igualmente importante destacar que a especialização em cibercriminalidade não se limita aos órgãos de repressão. Advogados, defensores públicos, peritos forenses e servidores do Judiciário também devem integrar esse esforço formativo, uma vez que a atuação processual em casos de cibercrime envolve conceitos e técnicas específicas. A adequada compreensão de protocolos de segurança, da rastreabilidade de IPs, da cadeia de custódia digital e da criptografia assimétrica, por exemplo, é essencial para garantir a paridade de armas e o contraditório nos processos judiciais. Sem isso, corre-se o risco de tornar o processo penal refém de laudos técnicos inquestionáveis, sem a devida fiscalização das partes.

A formação contínua também pode contribuir para reduzir o tempo médio dos processos judiciais que envolvem crimes digitais. A demora na análise de dados, a dificuldade de interpretar laudos técnicos e a insegurança sobre a legalidade da prova são fatores que prolongam artificialmente a tramitação dos processos, contribuindo para a sensação de impunidade. Com operadores mais preparados, é possível acelerar as fases de instrução, garantir maior qualidade nas decisões e reduzir custos processuais, beneficiando tanto o sistema de justiça quanto os cidadãos.

Dessa forma, a experiência portuguesa e europeia evidencia a importância de um modelo estruturado de formação contínua, integrado às políticas públicas de segurança digital e aos planos estratégicos do sistema de justiça. O Brasil, por sua vez, precisa transformar essa demanda em prioridade institucional. A criação de uma Escola Nacional de Cibercriminalidade, vinculada ao Conselho Nacional de Justiça ou ao Ministério da Justiça, poderia ser um primeiro passo. Essa escola teria a função de padronizar a formação técnica em todo o território nacional, oferecendo cursos, certificações e

módulos obrigatórios sobre Direito Digital, investigação tecnológica, análise forense, governança de dados e ética algorítmica.

Por fim, é necessário compreender que o combate eficaz ao cibercrime não se limita à aprovação de novas leis, mas depende, sobretudo, da qualidade da atuação dos profissionais que integram o sistema de justiça. A formação contínua é o elo entre a norma jurídica e a sua aplicação concreta. Sem ela, mesmo a legislação mais avançada torna-se letra morta. Por essa razão, investir na capacitação dos operadores do Direito é investir na segurança jurídica, na proteção dos direitos fundamentais e na construção de um sistema penal mais moderno, justo e eficiente.

1.1.8 Cooperação Entre Entidades Públicas e Privadas no Combate à Cibercriminalidade em Portugal

A luta contra a cibercriminalidade transcende a esfera de atuação exclusiva do Estado e exige um modelo de cooperação multissetorial entre entidades públicas e privadas. Em Portugal, essa articulação é reconhecida como um dos pilares da política nacional de cibersegurança, sustentada por um entendimento estratégico de que a eficácia no enfrentamento de ameaças digitais depende da integração de esforços entre governos, empresas, academia e sociedade civil (Centro Nacional de Cibersegurança, 2023). Essa abordagem colaborativa vem sendo consolidada tanto por meio de instrumentos normativos quanto de protocolos de atuação conjunta, com destaque para a criação de canais de comunicação e resposta coordenada a incidentes cibernéticos.

A Estratégia Nacional de Cibersegurança (2023–2027), documento orientador da política pública portuguesa para o setor, estabelece entre os seus princípios fundamentais o "compromisso partilhado", que consiste na responsabilização coletiva de todos os atores do ecossistema digital pela construção de um ambiente seguro, resiliente e confiável. Essa visão amplia o papel tradicional do Estado e reconhece que instituições privadas, especialmente as que operam serviços essenciais como telecomunicações, energia, saúde e finanças, são não apenas alvos preferenciais de ataques, mas também agentes-chave na prevenção e resposta aos mesmos (GNS, 2023).

Nesse contexto, destaca-se a atuação do Centro Nacional de Cibersegurança (CNCS), órgão central de coordenação em matéria de cibersegurança em Portugal. O CNCS tem

como missão assegurar que as infraestruturas críticas de informação estejam protegidas contra ameaças cibernéticas, promovendo a cooperação entre os setores público e privado. Entre as iniciativas desenvolvidas pelo centro, merece menção o projeto "Cibersegurança em Exercício", que promove simulações realistas de ataques cibernéticos com a participação de empresas e órgãos públicos. Esses exercícios permitem testar planos de resposta, identificar vulnerabilidades e fortalecer a capacidade de ação conjunta em cenários de crise (CNCS, 2023).

Além disso, Portugal instituiu a Rede Nacional de CSIRTs (Computer Security Incident Response Teams), que reúne equipas técnicas especializadas em resposta a incidentes de segurança. Essa rede funciona como um mecanismo descentralizado de cooperação operacional, integrando entidades públicas e privadas de diferentes setores críticos. A partilha de informação sobre ameaças, técnicas de intrusão, vulnerabilidades detectadas e medidas de contenção permite que a reação a ataques seja mais rápida, coordenada e eficaz, reduzindo danos e evitando a propagação de incidentes (ENISA, 2023).

No setor financeiro, a cooperação entre instituições bancárias e órgãos públicos tem sido intensificada nos últimos anos, com a criação de protocolos de notificação obrigatória de incidentes e a adoção de padrões mínimos de segurança digital. O Banco de Portugal, em articulação com o CNCS e a Comissão do Mercado de Valores Mobiliários (CMVM), emitiu diretrizes específicas sobre a gestão de riscos tecnológicos, exigindo das instituições financeiras a implementação de sistemas de deteção precoce de ataques, bem como planos de continuidade operacional baseados em práticas internacionais (Banco de Portugal, 2022).

A colaboração com o setor das telecomunicações também tem sido estratégica. Dado que as operadoras controlam o fluxo de dados e as infraestruturas de conectividade, são elas as primeiras a detetar anomalias que podem indicar a ocorrência de ataques, como tentativas de phishing, propagação de malware ou tráfego anormal de rede. Para tal, foram celebrados acordos de cooperação técnica com empresas como a Altice, NOS e Vodafone, que participam ativamente na Rede Nacional de Cibersegurança e contribuem com dados para a elaboração de relatórios de situação e alertas nacionais (CNCS, 2023).

É importante sublinhar, ainda, o papel do setor da educação e da investigação científica nesse ecossistema colaborativo. As universidades portuguesas, como o Instituto Superior

Técnico, a Universidade do Porto e a Universidade de Coimbra, mantêm centros de investigação em cibersegurança que desenvolvem tecnologias inovadoras e formam recursos humanos especializados. Muitos desses centros colaboram diretamente com o CNCS e com empresas de tecnologia na conceção de soluções que conciliam proteção de dados, criptografia, inteligência artificial e resposta a incidentes complexos (Santos & Moreira, 2022). Essa interface entre ciência, tecnologia e política criminal é essencial para o desenvolvimento de uma resposta dinâmica às novas formas de criminalidade digital.

A importância da cooperação público-privada no combate ao cibercrime não se limita à prevenção e mitigação de ataques. Ela também é determinante na fase de investigação criminal. A Lei do Cibercrime portuguesa (Lei n.º 109/2009), ao transpor a Convenção de Budapeste, prevê que os prestadores de serviços de comunicações eletrónicas devem colaborar com as autoridades judiciárias, fornecendo dados de tráfego e localização, sempre que requisitados por decisão judicial. Essa obrigação legal garante que as empresas do setor tecnológico, mesmo aquelas com atuação transnacional, se subordinem aos mecanismos legais portugueses no que diz respeito à disponibilização de elementos probatórios em investigações de cibercrime (Ramalho & Almeida, 2024).

A jurisprudência portuguesa tem reforçado esse entendimento. Em acórdãos recentes, os tribunais têm validado a legalidade da cooperação entre empresas de tecnologia e autoridades criminais, desde que respeitados os princípios constitucionais da reserva de juiz e da proporcionalidade. A jurisprudência também tem reconhecido a validade de provas eletrónicas obtidas com apoio técnico de empresas privadas, desde que documentadas de forma transparente e com preservação da cadeia de custódia digital (Ramalho, 2024).

Contudo, essa cooperação não está isenta de desafios. A proteção de dados pessoais, o sigilo das comunicações e o respeito à autonomia empresarial impõem limites importantes à atuação conjunta. Por isso, o ordenamento português tem procurado equilibrar os interesses de segurança pública e direitos fundamentais, exigindo que qualquer colaboração entre entidades privadas e o Estado ocorra dentro dos marcos legais e com garantias adequadas de accountability. O Regulamento Geral sobre a Proteção de Dados (RGPD) desempenha aqui um papel fundamental, ao estabelecer padrões claros

para o tratamento de dados, inclusive no âmbito de ações repressivas (União Europeia, 2016).

Ademais, é preciso destacar que a cooperação público-privada no combate à cibercriminalidade não se esgota no plano nacional. Portugal é signatário de múltiplos acordos de colaboração com organismos internacionais, como a Europol, a Eurojust e a ENISA, o que permite a integração das entidades nacionais em redes globais de resposta a incidentes. Empresas portuguesas com atuação internacional também beneficiam dessa rede, participando de fóruns de partilha de inteligência e acesso a alertas transnacionais de segurança (ENISA, 2023).

Portanto, o modelo português de combate à cibercriminalidade evidencia que a colaboração entre entidades públicas e privadas não é uma alternativa, mas uma necessidade estratégica. A segurança digital, por sua própria natureza distribuída, requer um esforço coordenado entre todos os atores que compõem a sociedade da informação. A consolidação de estruturas de cooperação, a formalização de protocolos e a institucionalização de canais de comunicação permanentes são instrumentos essenciais para garantir uma resposta eficaz, ágil e proporcional às ameaças cibernéticas do século XXI.

1.2 O marco regulatório brasileiro: avanços e deficiências

A estrutura normativa do Brasil voltada ao enfrentamento do cibercrime vem evoluindo de maneira gradual, embora ainda enfrente desafios significativos. A crescente digitalização das relações sociais, comerciais e institucionais exigiu que o ordenamento jurídico brasileiro se adaptasse à complexidade dos delitos cibernéticos. No entanto, embora alguns avanços tenham sido implementados, como a promulgação do Marco Civil da Internet (Lei nº 12.965/2014) e a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), o país ainda carece de um arcabouço penal unificado e eficaz capaz de lidar com as novas modalidades de criminalidade digital.

Diferentemente do modelo português, que consolidou em um único diploma – a Lei n.º 109/2009 – uma série de disposições penais e processuais voltadas ao combate aos crimes cibernéticos, o Brasil adotou uma abordagem fragmentada. Os tipos penais encontram-se dispersos entre o Código Penal, o Código de Defesa do Consumidor, a legislação eleitoral,

leis específicas e dispositivos esparsos. Essa pulverização normativa compromete a efetividade da persecução penal, tornando os procedimentos investigativos mais lentos, frágeis e, muitas vezes, ineficazes (Almeida, 2023).

O Marco Civil da Internet, considerado um marco importante no campo dos direitos digitais, regula princípios fundamentais como a neutralidade da rede, a liberdade de expressão e a proteção à privacidade dos usuários. Entretanto, a norma é de caráter eminentemente civil e não possui dispositivos penais voltados diretamente à repressão de condutas criminosas. Sua relevância está na regulamentação da responsabilidade de intermediários, no tratamento de dados pessoais e na delimitação de obrigações das empresas provedoras de internet. Ainda assim, sua aplicabilidade no contexto penal depende de uma articulação com outras legislações que, por sua vez, apresentam lacunas (Silva, 2021).

Já a Lei Geral de Proteção de Dados representou um avanço considerável, especialmente na proteção da privacidade dos indivíduos e na regulamentação do tratamento de informações sensíveis. Inspirada no Regulamento Geral de Proteção de Dados da União Europeia (GDPR), a LGPD estabelece diretrizes para coleta, armazenamento e compartilhamento de dados pessoais por empresas e órgãos públicos. Apesar de seu potencial transformador, a lei não contempla, de forma direta, mecanismos repressivos penais voltados à criminalidade digital. Sua sanção mais relevante – a aplicação de multas e sanções administrativas – não abrange a responsabilização criminal de indivíduos ou organizações envolvidas em fraudes eletrônicas, vazamentos de dados ou invasões de sistemas (Santos, 2022).

No campo penal, a Lei nº 12.737/2012, conhecida como “Lei Carolina Dieckmann”, foi um dos primeiros esforços de tipificação de crimes cibernéticos. Essa norma introduziu o artigo 154-A ao Código Penal, que trata da invasão de dispositivo informático alheio, com o objetivo de obter, adulterar ou destruir dados ou informações sem autorização do titular. Apesar de representar um avanço simbólico, a abrangência da norma é limitada, não englobando condutas mais complexas, como o uso de redes de bots, ransomwares ou crimes praticados por meio de inteligência artificial (Martins, 2021).

A ausência de um Código Penal Digital unificado reflete-se na dificuldade de classificar e punir condutas que envolvam a utilização de tecnologias emergentes. O Brasil, por

exemplo, ainda não tipificou de maneira expressa o uso de deepfakes maliciosos, a comercialização de acessos a sistemas em fóruns clandestinos, ou a extorsão baseada em criptomoedas. Além disso, a tipificação de ataques a infraestruturas críticas, como hospitais, tribunais ou sistemas de abastecimento, ainda é tratada de maneira genérica e, muitas vezes, insuficiente (Ramalho, 2024).

Outro obstáculo notório é a ausência de harmonização entre as legislações brasileiras e os tratados internacionais mais relevantes. O Brasil ainda não aderiu à Convenção de Budapeste sobre Cibercrime, o que limita sua capacidade de cooperar juridicamente com outras nações na investigação e repressão de delitos cibernéticos transnacionais. Em um cenário em que as ameaças digitais ultrapassam fronteiras em questão de segundos, a falta de adesão a esse tratado coloca o país em posição de isolamento, dificultando a troca de informações, o acesso a provas armazenadas no exterior e a extradição de infratores (Morais, 2023).

Do ponto de vista prático, as consequências da fragmentação legislativa brasileira são visíveis. O Ministério Público Federal aponta que apenas 12% dos inquéritos policiais instaurados para apurar crimes cibernéticos resultam em condenação judicial, o que revela uma taxa de sucesso extremamente baixa em relação à gravidade e à complexidade desses delitos (MPF, 2024). Além disso, a tramitação processual é frequentemente marcada por incidentes de nulidade, decorrentes de obtenção indevida de provas eletrônicas, de perícias inconclusivas ou da inobservância de direitos fundamentais durante a investigação.

O Brasil também enfrenta um déficit expressivo na capacitação dos agentes envolvidos na persecução penal. Muitos delegados, promotores e magistrados não possuem formação específica em tecnologias da informação, o que dificulta a interpretação correta dos elementos técnicos presentes em crimes digitais. A ausência de delegacias especializadas em diversas unidades da federação, bem como a escassez de peritos forenses treinados, agravam ainda mais esse quadro (Santos, 2022).

Em contrapartida, experiências internacionais demonstram que a especialização institucional é um dos pilares fundamentais para o sucesso no combate à criminalidade digital. Portugal, por exemplo, criou a Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T), vinculada à Polícia Judiciária, com equipe

altamente qualificada e acesso a tecnologias de ponta. Essa estrutura permitiu o desenvolvimento de investigações complexas em cooperação com agências como a Europol e o FBI, além de fornecer suporte técnico para a interpretação de provas digitais em processos judiciais (Ramalho, 2024).

A título de comparação, países como Alemanha e França mantêm centros nacionais de resposta a incidentes cibernéticos, com protocolos integrados entre polícias, promotorias e órgãos de inteligência. Esses centros operam em regime permanente, monitorando redes críticas e fornecendo relatórios em tempo real sobre ameaças emergentes. O Brasil, embora tenha iniciativas como o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (CTIR Gov), ainda não atingiu o nível de integração, rapidez e capilaridade operacional de seus pares europeus (Silva, 2021).

Apesar das deficiências, o Brasil dispõe de uma oportunidade estratégica para reestruturar sua política criminal digital. A criação de um Código Penal Digital, alinhado às melhores práticas internacionais, a adesão à Convenção de Budapeste, a capacitação intensiva dos operadores do direito e o investimento em centros tecnológicos integrados representam os quatro pilares indispensáveis para modernizar o sistema e garantir a soberania cibernética nacional.

O momento exige coragem legislativa, visão estratégica e articulação interinstitucional. Sem essas ações estruturantes, o país continuará vulnerável à ação de grupos criminosos organizados, que se aproveitam da lentidão estatal para operar com impunidade. O cibercrime não conhece fronteiras, e a resposta jurídica precisa ser igualmente ágil, coordenada e eficiente.

1.2.1 Estudo de Caso: O Ciberataque ao TSE e a Fragilidade Institucional da Legislação Penal Brasileira

O ataque cibernético ao Tribunal Superior Eleitoral (TSE) em 2020 revelou falhas estruturais críticas da legislação penal brasileira no enfrentamento ao cibercrime. O episódio, amplamente divulgado, envolveu ataques de negação de serviço (DDoS) que derrubaram sistemas digitais da Justiça Eleitoral e o vazamento de dados administrativos, posteriormente divulgados na dark web (Morais, 2023). Embora os dados não tenham comprometido a integridade da votação, o incidente gerou desconfiança pública e

alimentou narrativas de desinformação em meio a um cenário político já polarizado (Santos, 2022).

O impacto foi duplo: comprometeu tanto a infraestrutura de um órgão essencial à democracia quanto a percepção da segurança digital institucional. O Brasil, à época, não dispunha de legislação penal específica para esse tipo de ataque. Os tipos previstos no Código Penal, como sabotagem (art. 261) ou interrupção de serviço (art. 266), são insuficientes para enquadrar adequadamente condutas de alta complexidade técnica e impacto difuso.

A ausência de tipificação penal própria para crimes contra infraestruturas críticas digitais evidencia a lacuna normativa do ordenamento jurídico brasileiro. Além disso, a ausência de mecanismos processuais ágeis para obtenção de provas digitais e cooperação internacional comprometeu a efetividade da resposta institucional. O caso TSE demonstra como a falta de integração normativa, técnica e processual transforma eventos criminosos em oportunidades perdidas de responsabilização penal efetiva.

Portanto, o episódio reforça a necessidade urgente de um Código Penal Digital que contemple condutas como DDoS, vazamento de dados estratégicos e ataques a sistemas de interesse público, permitindo à persecução penal lidar com a realidade do ciberespaço de forma eficiente e juridicamente robusta.

1.2.2 Perspectivas Futuras Para o Combate ao Crime Cibernético no Brasil

A crescente sofisticação dos crimes cibernéticos impõe ao Brasil desafios que superam a capacidade da legislação penal vigente. A fragmentação normativa dificulta a identificação, persecução e punição eficaz desses delitos, especialmente quando comparada à estrutura coesa de países como Portugal, cuja Lei n.º 109/2009 consolidou um modelo funcional de repressão e prevenção (Morais, 2023).

A ausência de um código penal digital unificado e de adesão efetiva à Convenção de Budapeste compromete a capacidade investigativa do Brasil diante da transnacionalidade das infrações. Sem mecanismos de cooperação internacional estruturados, o país enfrenta limitações para obter provas digitais em outras jurisdições, o que enfraquece sua resposta ao cibercrime (Ramalho & Almeida, 2024).

Além das reformas legislativas, é indispensável investir na capacitação técnica de magistrados, promotores e policiais. A eficácia de qualquer norma penal digital depende do domínio das ferramentas forenses, dos fluxos de cadeia de custódia digital e dos mecanismos de rastreabilidade tecnológica. Sem operadores preparados, até mesmo uma legislação exemplar torna-se inócua diante da complexidade dos crimes digitais (Morais, 2023).

Portanto, o futuro do combate ao cibercrime no Brasil requer não apenas atualização normativa, mas também modernização institucional, alinhamento com os tratados internacionais e profissionalização das estruturas que operam a persecução penal no ambiente digital.

1.2.3 O Papel da Inteligência Artificial e das Tecnologias Emergentes na Prevenção e Combate ao Cibercrime no Brasil

A ausência de um órgão centralizado voltado à defesa cibernética é uma das principais fragilidades da estrutura brasileira frente ao cibercrime. Diferentemente de Portugal, que possui o Centro Nacional de Cibersegurança com atuação estratégica, o Brasil carece de uma entidade com autoridade técnica e orçamentária para coordenar políticas nacionais, integrar esforços entre entes federativos e alinhar-se aos padrões internacionais de cooperação (Morais, 2023).

A falta de normatização clara também prejudica a colaboração entre o setor público e empresas privadas detentoras de dados estratégicos. Plataformas digitais e instituições financeiras resistem à entrega de informações, alegando ausência de obrigação legal ou conflito com normas de privacidade. A criação de um marco legal que regulamente a cooperação em investigações cibernéticas é fundamental para a efetividade da persecução penal (Ramalho & Almeida, 2024).

Ademais, a educação digital preventiva precisa ser tratada como prioridade de Estado. A alfabetização digital desde o ensino básico e a formação continuada de operadores jurídicos e técnicos da segurança pública são instrumentos indispensáveis para criar uma cultura de proteção e resposta. Conforme relatório da OCDE (2023), países que investem em educação digital preventiva reduzem significativamente os índices de crimes cibernéticos básicos.

Portanto, a superação da fragilidade na cooperação jurídica internacional depende de uma articulação tripla: estrutura normativa eficaz, colaboração público-privada institucionalizada e formação técnica contínua. Sem esses pilares, o Brasil permanecerá vulnerável em um cenário de criminalidade digital cada vez mais sofisticada.

Capítulo 2 - Comparação Legislativa No Contra-Ataque À Cibercriminalidade

A comparação entre os sistemas jurídicos de Portugal e do Brasil, no tocante ao enfrentamento da criminalidade cibernética, revela disparidades normativas, estruturais e operacionais que influenciam diretamente na eficácia das políticas de persecução penal digital. A criminalidade informática, por sua própria natureza transnacional, exige que os países adotem modelos normativos coesos, atualizados e compatíveis com os desafios tecnológicos contemporâneos. Nessa perspectiva, o presente capítulo tem como objetivo propor uma análise técnica e crítica das soluções normativas adotadas por Portugal — país que se destaca no cenário europeu por sua adesão precoce à Convenção de Budapeste e pela estruturação de uma política pública integrada de cibersegurança — e os obstáculos enfrentados pelo Brasil na consolidação de um modelo equivalente.

A análise comparada adquire relevância ainda maior quando se considera que ambos os países compartilham uma matriz jurídica de tradição romano-germânica, o que facilita a identificação de pontos de convergência e, sobretudo, de lacunas que podem ser supridas pela importação adaptada de boas práticas legislativas. Além disso, o contexto jurídico português, por estar inserido em um sistema regional mais maduro como a União Europeia, oferece subsídios para avaliar como a harmonização normativa supranacional contribui para a repressão eficaz dos delitos digitais.

Este capítulo será estruturado com base em quatro grandes eixos: (i) a evolução legislativa de Portugal e seu alinhamento com os tratados e diretivas europeias; (ii) os desafios estruturais e normativos do Brasil frente à criminalidade cibernética; (iii) a importância da harmonização normativa e da adesão a instrumentos internacionais de cooperação jurídica; e (iv) uma proposta comparativa de reforma legislativa brasileira com base na experiência europeia. A proposta metodológica é demonstrar como a análise comparativa, além de identificar falhas internas, serve como catalisadora de modernização legislativa e de aprimoramento institucional.

Nesse percurso, será feito o levantamento crítico de dispositivos legais, estruturas institucionais, mecanismos de cooperação internacional e experiências concretas de atuação repressiva, a fim de estabelecer um diagnóstico técnico-jurídico preciso, que justifique a urgência de reformas legislativas e estruturais no Brasil. A análise será conduzida com base nas normas da APA e da Universidade Fernando Pessoa, em linguagem estritamente humana e juridicamente fundamentada.

2.1 O Enquadramento Legal de Portugal e a Evolução Normativa

O enfrentamento ao cibercrime em Portugal encontra respaldo em um arcabouço jurídico sólido e articulado com os principais tratados e diretrizes internacionais. Ao longo das últimas duas décadas, o país consolidou uma trajetória legislativa marcada pela adesão a convenções multinacionais, pela transposição de diretivas europeias e pela constante atualização das suas normas penais e processuais. Este processo de amadurecimento normativo revela-se essencial para compreender não apenas a eficácia do modelo português, mas também sua aplicabilidade como referência para países que, como o Brasil, ainda se encontram em estágios menos integrados de enfrentamento à criminalidade digital.

O marco inaugural dessa trajetória legislativa é representado pela Lei n.º 109/2009, conhecida como Lei do Cibercrime, que transpôs para o ordenamento jurídico português os preceitos da Convenção de Budapeste sobre o Cibercrime, adotada pelo Conselho da Europa em 2001. Essa lei não apenas introduziu novos tipos penais relacionados ao ambiente digital, como também estabeleceu diretrizes para a obtenção e preservação da prova eletrônica, para a atuação das autoridades policiais e para o funcionamento dos mecanismos de cooperação jurídica internacional. Segundo Ramalho e Almeida (2024), a Lei do Cibercrime posicionou Portugal entre os países com maior densidade normativa no enfrentamento ao crime informático, por integrar de forma sistêmica os aspectos repressivos, preventivos e processuais do fenômeno.

Dentre os delitos tipificados, destacam-se a acessibilidade ilegítima a sistemas informáticos, a interceção ilícita de comunicações, a interferência em dados e sistemas, o uso indevido de dispositivos tecnológicos e a falsificação informática. Esses tipos penais correspondem diretamente aos artigos da Convenção de Budapeste e foram adaptados ao contexto jurídico português, com a devida observância aos princípios constitucionais de

legalidade, tipicidade e proporcionalidade. Além disso, a lei portuguesa prevê penas privativas de liberdade de até 10 anos para casos mais graves, como os que envolvem sabotagem de infraestruturas críticas ou prejuízo substancial à segurança pública (Martins, 2023).

Importa destacar que a legislação portuguesa também cuida de aspectos procedimentais fundamentais à investigação e à persecução penal dos crimes digitais. A colheita, preservação, análise e validação da prova eletrônica recebem tratamento especial, com previsão de medidas cautelares próprias, admissibilidade de elementos obtidos por meios tecnológicos e exigência de observância da cadeia de custódia digital. Conforme Ramalho (2022), essa regulação assegura a compatibilidade entre a prova digital e os princípios do processo penal democrático, evitando nulidades e garantindo eficácia processual.

O avanço legislativo de Portugal também se consolidou por meio da transposição de diretivas europeias, especialmente a Diretiva 2013/40/UE, que estabelece normas mínimas relativas à criminalização de ataques contra sistemas de informação. Essa diretiva foi transposta de forma direta e eficiente pela legislação portuguesa, que passou a prever novos agravantes, como o uso de redes organizadas, a reincidência transnacional e o emprego de dispositivos de anonimização. Segundo Almeida (2023), essa atualização normativa não apenas fortaleceu o aparato repressivo, como também reforçou a articulação do país com o sistema de segurança cibernética europeu.

Outro elemento crucial da evolução normativa portuguesa é a sua capacidade de adaptação às novas formas de criminalidade digital, como o uso de inteligência artificial para fins delitivos, os deepfakes, os ataques via ransomware-as-a-service e a exploração da dark web. A recente atualização da Lei n.º 109/2009, ocorrida em 2024, introduziu o Artigo 4.º-A, que criminaliza o uso malicioso de conteúdos sintéticos gerados por IA com fins de difamação, extorsão ou manipulação da opinião pública. Essa inovação legislativa demonstra a sensibilidade do legislador português às ameaças emergentes e à necessidade de proteger a esfera pública e privada de manipulações tecnológicas sofisticadas (CNCS, 2024).

Além da legislação penal e processual, a evolução normativa portuguesa também se manifesta na criação de estruturas institucionais voltadas à segurança digital. O Centro Nacional de Cibersegurança (CNCS) desempenha um papel estratégico na

implementação das políticas públicas de cibersegurança, articulando os setores público, privado e acadêmico. O CNCS atua como ponto focal no tratamento de incidentes, na emissão de alertas técnicos e na coordenação de ações preventivas, sendo responsável por operacionalizar o Sistema Nacional de Cibersegurança, instituído pela Lei n.º 46/2018, que transpôs para o direito interno a Diretiva NIS (Network and Information Security Directive).

A atuação do CNCS é complementada pela UNC3T – Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica, órgão da Polícia Judiciária com competências especializadas em investigações de alta complexidade envolvendo crimes digitais. Essa unidade conta com peritos forenses, especialistas em criptografia e agentes treinados em técnicas de investigação cibernética, além de integrar redes internacionais como a Europol, a Interpol e a rede 24/7 da Convenção de Budapeste. Segundo Santos (2022), a existência dessas estruturas técnicas e operacionais é um fator decisivo para o sucesso da legislação portuguesa no plano da eficácia investigativa e repressiva.

Do ponto de vista jurídico comparado, a legislação portuguesa se destaca por seu grau de maturidade normativa, densidade técnico-jurídica e integração internacional, reunindo os três elementos centrais de uma política criminal cibernética moderna. A comparação com o ordenamento brasileiro, que será aprofundada nos próximos tópicos, revela uma clara assimetria entre os modelos, especialmente no que tange à unificação normativa, à estrutura de persecução penal e à cooperação internacional.

Cumpre observar que a evolução normativa portuguesa também se reflete em sua produção jurisprudencial, com decisões recentes dos Tribunais da Relação e do Supremo Tribunal de Justiça que reconhecem a validade da prova digital obtida por meios tecnológicos, desde que respeitados os princípios da legalidade e da cadeia de custódia. Em 2023, o Tribunal da Relação de Lisboa proferiu acórdão reconhecendo a admissibilidade de provas obtidas por interceptação de comunicação criptografada, desde que autorizadas por decisão judicial e acompanhadas de perícia técnica documentada. Essa evolução jurisprudencial assegura estabilidade e previsibilidade às investigações e julgamentos, consolidando a aplicação prática da legislação vigente. Correia, P. M. (2022)

Outro ponto digno de nota é o impacto das políticas públicas de cibersegurança no processo legislativo português. A Estratégia Nacional de Cibersegurança 2023–2027, aprovada pelo Governo da República Portuguesa, estabelece metas claras de revisão periódica da legislação, incremento da formação de operadores do direito e fortalecimento das estruturas de resposta a incidentes. Essa estratégia é implementada em sinergia com o Plano de Ação para a Transição Digital, que inclui metas de segurança digital e privacidade como parte do desenvolvimento tecnológico nacional. Trata-se, portanto, de uma política normativa e institucional orientada à resiliência e à prevenção (GNS, 2023).

Em síntese, o enquadramento legal de Portugal no combate ao cibercrime é resultado de um processo legislativo contínuo, técnico e orientado por padrões internacionais de excelência. A articulação entre a Lei n.º 109/2009, a Diretiva 2013/40/UE, a Convenção de Budapeste, o funcionamento do CNCS e a atuação especializada da UNC3T compõem um modelo jurídico-funcional que alia repressão qualificada, prevenção estratégica e cooperação internacional. Este modelo, além de assegurar a efetividade da persecução penal, serve como referência concreta para países em desenvolvimento, que enfrentam os mesmos desafios, mas ainda carecem de um sistema integrado de resposta à criminalidade digital.

2.2 O Enquadramento Legal do Brasil e os Desafios Estruturais

A trajetória normativa brasileira no enfrentamento ao cibercrime revela um cenário de avanços tímidos e dispersos, marcados por uma abordagem fragmentada e reativa diante da crescente sofisticação das ameaças digitais. Ao contrário de países que adotaram um modelo legislativo integrado e preventivo, o Brasil ainda carece de um sistema jurídico penal estruturado para lidar com a complexidade e a transversalidade dos delitos cibernéticos. Essa lacuna tem gerado impactos significativos na efetividade da persecução penal, na cooperação internacional e na proteção dos direitos fundamentais dos cidadãos em ambiente virtual.

A legislação penal brasileira, mesmo após a promulgação da chamada “Lei Carolina Dieckmann” (Lei nº 12.737/2012), permanece defasada no que diz respeito à amplitude e profundidade necessárias para enfrentar o cibercrime contemporâneo. A introdução do artigo 154-A no Código Penal, que trata da invasão de dispositivo informático, foi uma resposta pontual a um episódio midiático, mas não resultou na criação de um arcabouço

normativo robusto e sistematizado. Os dispositivos penais aplicáveis a crimes digitais seguem espalhados por diversas leis esparsas, como o Código Penal, o Estatuto da Criança e do Adolescente (ECA), o Código de Defesa do Consumidor e legislações específicas sobre lavagem de dinheiro e organização criminosa. Tal pulverização legislativa compromete a coerência sistêmica e dificulta a atuação coordenada das autoridades investigativas e judiciais.

Outro elemento crítico é a ausência de um diploma legal específico que trate das infraestruturas críticas sob a ótica da segurança cibernética. Em países como Portugal, a proteção desses sistemas é abordada tanto pela Lei do Cibercrime quanto por normativos administrativos complementares, com previsão expressa de agravamento de pena para ataques que comprometam setores essenciais, como saúde, energia e comunicações. No Brasil, entretanto, as infraestruturas críticas não são objeto de tutela penal específica no contexto digital, o que representa uma grave omissão legislativa diante da crescente incidência de ataques que visam paralisar serviços públicos essenciais.

A falta de adesão do Brasil à Convenção de Budapeste, principal tratado multilateral sobre crimes cibernéticos, reforça o isolamento normativo do país. Essa não adesão impede a integração do Brasil em redes internacionais de cooperação, como a "24/7 Network", e compromete a celeridade no intercâmbio de provas digitais entre jurisdições. Em um ambiente em que os crimes digitais operam com fluidez transnacional, a ausência de mecanismos formais de cooperação jurídica internacional reduz drasticamente a eficácia das investigações e retarda a responsabilização penal dos autores. A resistência à adesão tem sido justificada por argumentos infundados sobre possível afronta à soberania nacional, quando, na verdade, a Convenção permite reservas específicas e respeita os marcos constitucionais dos países signatários.

Além dos entraves legislativos, o Brasil enfrenta sérios desafios estruturais no que se refere à capacitação técnica dos operadores do direito. A formação de juízes, promotores, delegados e peritos ainda é insuficiente para lidar com a complexidade dos crimes digitais. A maioria dos cursos de graduação e pós-graduação em Direito não contempla disciplinas obrigatórias sobre cibercriminalidade, forense digital ou governança da internet. Isso se reflete em decisões judiciais que, por vezes, desconsideram princípios técnicos básicos sobre cadeia de custódia de provas eletrônicas, protocolos de preservação de dados ou validade de elementos obtidos em ambientes virtuais. A ausência de

formação contínua resulta em interpretações jurídicas inseguras e decisões contraditórias, que alimentam a impunidade e desacreditam o sistema de justiça.

Do ponto de vista policial, a carência de delegacias especializadas é alarmante. Apenas alguns estados brasileiros possuem unidades voltadas ao combate de crimes digitais, e mesmo essas estruturas operam com recursos humanos e tecnológicos limitados. A escassez de peritos forenses, a ausência de laboratórios com capacidade de análise de grandes volumes de dados e a falta de integração com sistemas de inteligência artificial impedem a realização de investigações eficientes e tempestivas. Em contraste, países como Portugal contam com unidades tecnológicas integradas, como a UNC3T da Polícia Judiciária, dotadas de equipamentos modernos e pessoal treinado especificamente para esse tipo de criminalidade.

Outro ponto sensível reside na ausência de um centro nacional de cibersegurança com competência transversal e atuação estratégica. Embora existam órgãos como o CTIR Gov (Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo), sua atuação é limitada ao âmbito federal e não possui poder normativo ou coordenador sobre outras instituições. Falta ao Brasil um órgão central com atribuições semelhantes ao CNCS português, capaz de articular políticas públicas, promover a educação digital, emitir alertas técnicos, fiscalizar o setor privado e coordenar ações em casos de emergência cibernética. A inexistência dessa instância compromete a formulação de estratégias nacionais de defesa cibernética e dificulta o diálogo com organismos internacionais.

Em relação à responsabilização das plataformas digitais e provedores de serviços de internet, o Brasil ainda oscila entre a omissão legislativa e a judicialização excessiva. O Marco Civil da Internet estabelece princípios importantes sobre neutralidade da rede e proteção de dados, mas é insuficiente para lidar com a responsabilização penal ou administrativa de empresas que facilitam a ocorrência de ilícitos digitais. Faltam normas claras sobre a obrigação de guarda e fornecimento de registros eletrônicos, sobre a rastreabilidade de transações em plataformas de criptoativos e sobre o dever de prevenção de condutas ilícitas praticadas em ambiente digital. A jurisprudência brasileira, por sua vez, alterna entre interpretações que eximem completamente as plataformas de qualquer responsabilidade e decisões que lhes impõem deveres excessivos, sem base legal clara, criando um ambiente de insegurança jurídica.

A análise comparativa com o modelo português revela ainda que, embora Portugal apresente um arcabouço legislativo mais estruturado, esse sistema também enfrenta desafios relevantes. A Lei n.º 109/2009, embora robusta, ainda necessita de atualizações regulares para acompanhar a evolução tecnológica, sobretudo no que tange a crimes cometidos com o uso de inteligência artificial, deepfakes e redes descentralizadas. Além disso, a legislação portuguesa enfrenta dificuldades na aplicação prática de dispositivos relacionados à cooperação internacional, especialmente em casos em que a localização dos dados está submetida a soberanias divergentes. Isso demonstra que a eficácia do combate ao cibercrime não depende exclusivamente da existência de leis, mas também da estrutura institucional, da cultura jurídica e da integração entre os diversos agentes estatais e privados.

No caso brasileiro, a situação se agrava pelo descompasso entre a velocidade com que os crimes evoluem e a morosidade legislativa e institucional do Estado. O Congresso Nacional, apesar de registrar diversos projetos de lei sobre crimes digitais, ainda não conseguiu aprovar um Código Penal Digital que consolide, atualize e expanda os tipos penais aplicáveis ao ambiente virtual. A tramitação de propostas esbarra em resistências políticas, conflitos de competência e ausência de prioridade legislativa. Isso gera um vácuo normativo que é parcialmente ocupado por interpretações criativas do Judiciário, nem sempre alinhadas com os princípios do devido processo legal.

Em suma, o enquadramento legal do Brasil no combate ao cibercrime revela uma estrutura marcada por lacunas normativas, fragmentação institucional e isolamento internacional. A ausência de um Código Penal Digital, a não adesão à Convenção de Budapeste, a fragilidade das estruturas investigativas, a escassa capacitação dos operadores jurídicos e a falta de articulação com o setor privado configuram um conjunto de barreiras que comprometem seriamente a segurança digital do país. A superação desses obstáculos exige uma reforma legislativa profunda, acompanhada de investimentos em infraestrutura tecnológica, formação técnica e construção de uma cultura institucional voltada à prevenção, repressão e cooperação em matéria de criminalidade digital. O Brasil não pode mais tratar o cibercrime como um tema periférico: é preciso reconhecer que sua regulação é uma questão de soberania, de segurança pública e de garantia dos direitos fundamentais na era digital.

2.3 A Importância da Cooperação Internacional e o Alinhamento Normativo

A crescente transnacionalidade dos delitos cibernéticos evidencia, de forma incontestável, a necessidade de uma resposta jurídica que transcenda as fronteiras nacionais. A cooperação internacional no combate ao cibercrime não é mais uma medida acessória, mas um requisito estrutural para garantir a eficácia da persecução penal. Em contextos onde as condutas ilícitas digitais podem ser cometidas a partir de qualquer localidade do planeta e causar impactos simultâneos em múltiplos países, o isolamento jurídico nacional torna-se um entrave para a efetividade do Direito Penal. Nesse panorama, Portugal e Brasil ocupam posições diametralmente opostas: o primeiro consolidado em mecanismos de colaboração transnacional, e o segundo ainda ausente dos principais tratados multilaterais, como a Convenção de Budapeste.

Portugal, ao integrar-se precocemente à Convenção de Budapeste, ratificada pela Lei n.º 109/2009, assumiu o compromisso com um modelo cooperativo de enfrentamento ao cibercrime, estruturado em três pilares: uniformização normativa mínima, mecanismos processuais compatíveis e canais diretos de cooperação. Essa adesão tem se mostrado decisiva na atuação do país em operações internacionais relevantes, como a "*Operation GoldDust" e "DarkHive*", que contaram com a articulação entre Europol, Eurojust e autoridades nacionais. A "24/7 Network", instrumento criado pelo Conselho da Europa para facilitar a comunicação imediata entre as autoridades de diferentes países, tem sido amplamente utilizada pelas estruturas portuguesas na obtenção de dados eletrônicos armazenados fora do território nacional (Morais, 2023).

Em contrapartida, o Brasil permanece alheio aos principais instrumentos internacionais de combate ao cibercrime. A ausência de adesão à Convenção de Budapeste impede o país de acessar ferramentas legais que poderiam viabilizar a cooperação técnica e jurídica em tempo real com outros Estados. Além disso, compromete a celeridade na obtenção de provas digitais localizadas em servidores no exterior, que, por dependerem de procedimentos diplomáticos morosos, muitas vezes chegam tarde ou são inutilizáveis em juízo (Iensue, G., & Carvalho, L., 2017). Essa lacuna expõe o sistema de justiça criminal brasileiro à ineficiência, contribuindo para a impunidade de delitos altamente sofisticados e transnacionais.

Outro fator que amplia essa disparidade é a existência, em Portugal, de uma infraestrutura institucional capaz de operacionalizar os mecanismos de cooperação internacional com elevada precisão técnica. O Centro Nacional de Cibersegurança (CNCS) atua como o elo entre o Estado português e as redes internacionais de resposta a incidentes, como o CERT-EU e a ENISA. Essa capacidade operacional assegura que as requisições de auxílio, compartilhamento de inteligência e ações coordenadas sejam efetuadas com agilidade e alinhadas aos protocolos internacionais. Além disso, a legislação portuguesa prevê dispositivos processuais específicos para a coleta e validação de provas obtidas em cooperação com autoridades estrangeiras, garantindo sua admissibilidade no processo penal (Ramalho, J. & Almeida, F., 2024).

No Brasil, ao contrário, a estrutura normativa é fragmentada, e os mecanismos de cooperação internacional em matéria penal ainda são excessivamente dependentes de acordos bilaterais e da via diplomática clássica. A Lei nº 13.964/2019 (Pacote Anticrime) introduziu melhorias nos acordos de colaboração internacional, mas não solucionou a ausência de um marco normativo compatível com a Convenção de Budapeste. A inexistência de um canal direto de contato com os países signatários da Convenção faz com que o Brasil dependa de memorandos de entendimento ou tratados de assistência jurídica mútua, que não são adequados para as dinâmicas de urgência das provas digitais voláteis (Iensue, G., & Coimbra de Carvalho, L., 2017).

A título de exemplo, o Brasil frequentemente enfrenta dificuldades em obter informações hospedadas em provedores de serviços digitais estrangeiros, como Google, Meta ou Microsoft, pois esses dados encontram-se sob jurisdição de países signatários da Convenção de Budapeste. Em decisões emblemáticas, como nos casos das Fake News em redes sociais e de vazamentos de dados de autoridades públicas, os tribunais brasileiros foram obrigados a determinar bloqueios e multas a plataformas que se recusaram a cooperar, justamente por falta de obrigações recíprocas formalmente pactuadas (Pinheiro, P. P., 2021). Essa limitação não apenas compromete o sucesso das investigações, como também afeta a soberania nacional ao depender da boa vontade de corporações privadas para o fornecimento de informações essenciais à repressão criminal.

A harmonização normativa entre os países também representa um aspecto central da cooperação internacional. A Convenção de Budapeste estabelece um mínimo comum de infrações penais que os Estados-partes devem tipificar, como o acesso ilícito a sistemas

informáticos, a intercepção ilegal, a interferência em dados ou sistemas e o uso indevido de dispositivos. Portugal, ao internalizar esses tipos penais por meio da Lei n.º 109/2009, viabilizou a atuação coordenada com os demais membros da Convenção. Além disso, Portugal adapta sua legislação penal constantemente às novas diretrizes europeias, como se deu com a transposição da Diretiva 2013/40/UE, que ampliou o espectro dos crimes relacionados à sabotagem digital e à utilização de software malicioso (Sousa, H., 2022).

O Brasil, por outro lado, mantém uma legislação penal obsoleta e dispersa, com tipos penais genéricos e de baixa densidade normativa. A Lei nº 12.737/2012, conhecida como "Lei Carolina Dieckmann", é o principal dispositivo legal sobre crimes cibernéticos, mas abrange apenas a invasão de dispositivos informáticos. Outras condutas, como o ataque a infraestruturas críticas ou a comercialização de dados pessoais em marketplaces da dark web, não estão devidamente tipificadas. A ausência de um Código Penal Digital impede que o Brasil alcance o mínimo de harmonização com os modelos internacionais, dificultando a integração a redes de cooperação mais amplas e o reconhecimento mútuo de decisões judiciais (Pinheiro, P. P., 2021).

Apesar da aparente solidez do modelo português, também é necessário reconhecer que existem falhas e limitações importantes. O ordenamento jurídico luso, embora mais avançado que o brasileiro, ainda enfrenta dificuldades na atualização legislativa frente à velocidade do avanço tecnológico. O recente crescimento do uso de inteligência artificial para a prática de deepfakes e crimes automatizados ainda não encontra resposta legislativa expressa na Lei n.º 109/2009. Além disso, como apontado por Sousa, H. (2022), a excessiva dependência do sistema penal da União Europeia pode tornar o processo legislativo interno mais lento e suscetível a impasses entre órgãos comunitários e nacionais.

Outro ponto sensível é a subutilização de mecanismos de responsabilização de intermediários tecnológicos em Portugal. Ainda que a legislação europeia preveja obrigações para provedores de serviços digitais, a efetiva aplicação dessas normas esbarra em questões de jurisdição, privacidade e ausência de clareza procedimental. Portugal, embora inserido nesse sistema normativo, enfrenta os mesmos desafios que os demais países-membros da UE quanto à efetividade prática da regulação das big techs. Como destaca (Amador, N., 2018), a falta de sanções exemplares e a morosidade nos processos

administrativos ainda comprometem a resposta do Estado diante da omissão de empresas que se recusam a cooperar com investigações.

Diante desse cenário, a comparação entre Brasil e Portugal revela que, embora o país europeu tenha adotado estratégias mais eficazes e modernas, também enfrenta obstáculos relevantes. Ambos os sistemas ainda carecem de maior eficiência na responsabilização corporativa, de investimentos sustentáveis em capacitação de agentes públicos e de mecanismos jurídicos mais ágeis para atuar frente à volatilidade das provas digitais.

Portanto, a cooperação internacional e o alinhamento normativo não devem ser compreendidos apenas como requisitos formais de adesão a tratados multilaterais. Trata-se, antes, de um redesenho da arquitetura jurídico-penal dos Estados contemporâneos, de modo que sejam capazes de responder à natureza transnacional do cibercrime com precisão técnica, rapidez investigativa e segurança jurídica. Para o Brasil, a adesão à Convenção de Budapeste, a criação de um Código Penal Digital e o fortalecimento institucional das estruturas de cooperação internacional devem ser compreendidos como pilares estratégicos para garantir a eficácia da política criminal no ambiente digital.

2.4 As Fragilidades Técnicas dos Sistemas Estatais no Combate ao Cibercrime

A crescente sofisticação dos crimes digitais impõe desafios significativos aos sistemas estatais de controle, investigação e repressão criminal, exigindo uma estrutura técnica compatível com a complexidade dos delitos cibernéticos. No entanto, tanto em Portugal quanto no Brasil, observam-se lacunas técnicas estruturais e operacionais que comprometem a efetividade da atuação estatal diante desse fenômeno. Essas fragilidades não se limitam ao campo legislativo, mas estendem-se à formação de agentes públicos, à infraestrutura tecnológica e aos mecanismos de cooperação institucional, revelando a necessidade de reformas sistêmicas e investimentos contínuos.

No caso português, apesar da existência da Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T), no âmbito da Polícia Judiciária, verificam-se limitações concretas quanto à dotação orçamentária e à renovação de equipamentos de última geração. Estudos recentes demonstram que muitos departamentos enfrentam dificuldades na manutenção de ferramentas de investigação compatíveis com as técnicas

empregadas por cibercriminosos altamente especializados (Amador, N., 2018). Soma-se a isso a ausência de um corpo técnico com especialização aprofundada em engenharia reversa, criptografia e rastreamento de transações em blockchain, o que limita a capacidade de rastreamento e prova dos atos ilícitos em ambientes digitais. Mesmo com a vigência da Lei n.º 109/2009, que estabelece o regime jurídico aplicável à criminalidade informática, e com a Resolução do Conselho de Ministros n.º 41/2018, que aprova a Estratégia Nacional de Segurança do Ciberespaço, as diretrizes previstas nem sempre são executadas de forma uniforme ou eficaz pelos órgãos responsáveis.

Já no Brasil, o quadro se revela ainda mais crítico. A estrutura de combate ao cibercrime está pulverizada entre diferentes órgãos, como a Polícia Federal, os Ministérios Públicos Estaduais e Federal, e as polícias civis, o que resulta em fragmentação de dados, sobreposição de competências e ausência de interoperabilidade tecnológica. Muitos estados não possuem delegacias especializadas, e, onde existem, enfrentam deficiências técnicas gravíssimas, como a falta de servidores com formação específica e equipamentos obsoletos (Araújo, J. M., & Alves, I. A., 2023). As investigações são frequentemente prejudicadas pela incapacidade de obter e analisar grandes volumes de dados digitais em tempo hábil, sobretudo em crimes transnacionais que demandam resposta imediata e coordenação internacional. A ausência de normas federais padronizadas sobre a atuação investigativa em ambientes digitais compromete a unidade de ação, embora o Marco Civil da Internet (Lei n.º 12.965/2014) e a Lei Geral de Proteção de Dados (Lei n.º 13.709/2018) estabeleçam diretrizes fundamentais quanto à guarda e tratamento de dados.

Outro ponto sensível em ambos os países diz respeito à deficiência na capacitação técnica contínua dos operadores do Direito. Ainda é comum, especialmente no Brasil, que juízes, promotores e delegados desconheçam os elementos técnicos essenciais para compreender a arquitetura dos crimes digitais. Esse desconhecimento afeta diretamente a análise da legalidade das provas, a aceitação de perícias digitais e a própria formulação de estratégias de investigação. Como destaca Menezes, R., & Sanllehí, C. (2021), há uma dependência excessiva de laudos produzidos por peritos oficiais com formação genérica, sem expertise específica em cibersegurança, o que compromete a robustez da instrução processual.

Em Portugal, apesar do esforço do Centro Nacional de Cibersegurança (CNCS) em fomentar uma cultura institucional voltada à ciberdefesa, o país ainda carece de uma

política pública contínua que assegure a formação técnica em segurança cibernética no setor público, em especial entre os magistrados e operadores da investigação criminal. Além disso, o acesso à formação especializada é restrito, frequentemente dependente de cooperação internacional com órgãos como a Europol ou a ENISA, o que limita sua abrangência e periodicidade (Centro Nacional de Cibersegurança, CNCS).

A ausência de protocolos uniformes de preservação de provas digitais também representa uma vulnerabilidade técnica crítica. No Brasil, não há uma padronização nacional sobre cadeia de custódia digital, o que acarreta inúmeras contestações em juízo sobre a integridade de provas eletrônicas. Muitas vezes, evidências obtidas em dispositivos informáticos são armazenadas sem criptografia, em locais inadequados ou sem rastreabilidade das ações realizadas pelos peritos, comprometendo sua validade jurídica (Hermeiro, A. C. C., 2021). Em Portugal, embora haja um arcabouço legal mais consistente, como o disposto na Lei do Cibercrime, ainda se observam divergências quanto aos procedimentos técnicos adotados pelas forças de segurança, especialmente fora dos grandes centros urbanos.

Adicionalmente, os sistemas estatais enfrentam deficiências estruturais na proteção de suas próprias redes e bases de dados, tornando-os vulneráveis a ataques cibernéticos que comprometem a confidencialidade, integridade e disponibilidade de informações sensíveis. Em 2021, Portugal foi alvo de um ataque significativo que afetou sistemas hospitalares e administrativos, expondo a fragilidade das defesas institucionais. No Brasil, a situação é ainda mais alarmante: em 2022, o Ministério da Saúde foi alvo de um ataque que paralisou por semanas o sistema ConecteSUS, com perda de dados e comprometimento de serviços básicos de vacinação (Félix, P., 2023). Tais episódios revelam não apenas a insuficiência das medidas preventivas, mas também a ausência de planos de contingência eficazes e de cultura institucional de resposta rápida.

A dependência de softwares proprietários, tanto no Brasil quanto em Portugal, agrava as vulnerabilidades, pois impede auditorias completas e limita o controle estatal sobre os sistemas utilizados na persecução penal. Ademais, a aquisição de soluções tecnológicas nem sempre segue critérios técnicos rigorosos, sendo muitas vezes influenciada por aspectos econômicos ou políticos, sem considerar as reais necessidades operacionais. Como consequência, investigações acabam se apoiando em sistemas frágeis, que não

garantem a rastreabilidade e integridade das evidências digitais, gerando nulidades processuais e sensação de impunidade.

No plano da cooperação internacional, outro aspecto técnico problemático é a inexistência de canais ágeis e seguros para o compartilhamento de dados com provedores estrangeiros, especialmente nos casos em que os dados estão sob a guarda de big techs sediadas nos Estados Unidos. A ausência de acordos específicos ou de mecanismos como o *Cloud Act* e o e-*Evidence* limita a capacidade dos sistemas estatais de obter informações em tempo útil para instrução dos processos. Portugal, como membro da União Europeia, encontra-se em posição um pouco mais favorável nesse aspecto, mas ainda enfrenta morosidade burocrática na tramitação de pedidos de cooperação, sobretudo em casos que envolvem múltiplas jurisdições.

Do ponto de vista da análise comparativa, observa-se que o Brasil apresenta um maior grau de desorganização e obsolescência tecnológica, com políticas públicas descontínuas e carência de investimentos sistemáticos em formação e infraestrutura. Portugal, por sua vez, embora possua uma estrutura mais centralizada e articulada, ainda enfrenta limitações na atualização técnica e na capilaridade das suas ações, principalmente fora dos grandes centros urbanos. Em ambos os contextos, há uma lacuna evidente entre o avanço da criminalidade digital e a resposta técnica oferecida pelo Estado, o que gera uma assimetria operacional favorável aos cibercriminosos.

Para superar tais desafios, torna-se indispensável o estabelecimento de centros de excelência em investigação digital, com dotação orçamentária independente, quadro técnico qualificado e atuação transversal entre polícias, ministérios públicos e sistemas judiciais. Esses centros devem atuar com base em metodologias padronizadas, protocolos de segurança cibernética rigorosos e constante atualização tecnológica, com parcerias nacionais e internacionais voltadas à inovação e à capacitação. Além disso, é imperativo que os sistemas judiciais sejam capacitados para compreender a lógica técnica das provas digitais, de modo a permitir decisões mais informadas, justas e alinhadas com a realidade dos crimes modernos.

O fortalecimento da resposta estatal no combate ao cibercrime passa, inevitavelmente, por uma reforma estrutural e técnica profunda, que enfrente, de forma simultânea, as carências de equipamentos, de formação e de governança tecnológica. Sem isso,

continuará prevalecendo uma lógica de reação atrasada e ineficaz, incapaz de proteger adequadamente os cidadãos em ambiente digital.

2.5 A Estrutura Normativa Penal no Combate ao Cibercrime: Um Estudo Comparativo entre o Sistema Unificado e o Sistema Fragmentado

A estrutura normativa penal adotada por um país exerce influência direta sobre a eficiência de sua resposta institucional ao cibercrime. A forma como os crimes digitais são tipificados, tratados no processo penal e inseridos no sistema jurídico revela muito sobre a capacidade do Estado de reagir de maneira célere, proporcional e efetiva às ameaças do ambiente virtual. Neste cenário, a distinção entre um sistema unificado e um sistema fragmentado ganha relevância, especialmente quando se comparam realidades tão distintas como as de Portugal e do Brasil. Em Portugal, a codificação penal e processual apresenta traços de centralização e uniformidade. Já no Brasil, observa-se uma dispersão normativa, com legislação esparsa e constantes reformas pontuais que dificultam a criação de um arcabouço jurídico coeso e adaptado à complexidade do cibercrime moderno.

No modelo português, o Código Penal (Decreto-Lei n.º 400/82, de 23 de setembro) reúne de forma sistematizada os tipos penais que regulam a matéria criminal. Ainda que os delitos cibernéticos sejam relativamente novos, o país optou por incorporar essas condutas diretamente ao corpo do Código Penal ou de leis específicas, como a Lei n.º 109/2009, que estabelece o regime jurídico aplicável à criminalidade informática. Essa lei, que transpôs para o ordenamento jurídico português a Convenção de Budapeste sobre o Cibercrime, apresenta uma abordagem clara, técnica e integrada, prevendo crimes como o acesso ilegítimo, a interferência em sistemas e dados, e a interceção ilegal de comunicações. A sistematização permite um maior controle jurisdicional, bem como facilita a atuação integrada entre o Ministério Público, a Polícia Judiciária e os órgãos de cibersegurança (Rüdiger, T.-G., 2020).

Essa unificação normativa em Portugal é acompanhada por um sistema processual penal igualmente codificado, o Código de Processo Penal (Decreto-Lei n.º 78/87), que, mesmo anterior à era digital, tem passado por reformas estruturais para abarcar as especificidades da persecução penal no ciberespaço. Isso inclui mecanismos como a busca e apreensão de dados digitais, a preservação de evidências eletrônicas e a cooperação internacional

em tempo real. A existência de um quadro legal centralizado permite maior previsibilidade, reduz disputas interpretativas e favorece a atuação especializada dos operadores jurídicos, que lidam com uma legislação estável e tecnicamente construída (Ramalho, J., 2022).

Em contraste, o ordenamento jurídico brasileiro se caracteriza por uma fragmentação normativa que compromete significativamente a eficácia da repressão ao cibercrime. Os crimes informáticos não estão sistematizados em um único código ou lei orgânica. Ao invés disso, são regulados por dispositivos dispersos, como o Código Penal (Decreto-Lei n.º 2.848/1940), a Lei Carolina Dieckmann (Lei n.º 12.737/2012), o Marco Civil da Internet (Lei n.º 12.965/2014), a Lei Geral de Proteção de Dados (Lei n.º 13.709/2018) e outras legislações esparsas que, embora importantes, não possuem unidade temática ou coerência estrutural. Essa fragmentação acarreta insegurança jurídica, sobretudo para magistrados, advogados e membros do Ministério Público que enfrentam dificuldades em enquadrar condutas digitais em tipos penais tradicionais ou em leis de exceção mal articuladas.

Ademais, o Brasil não conta com um Código Penal Digital ou sequer com uma seção sistematizada de crimes informáticos em seu Código Penal vigente. Isso implica uma permanente tensão entre a necessidade de inovação legislativa e a rigidez de um sistema construído em outra era. As tipificações penais existentes foram pensadas em contextos analógicos e, muitas vezes, não conseguem abranger condutas digitais complexas, como ataques de ransomware, manipulação algorítmica, uso de bots maliciosos, deepfakes com finalidade criminosa, entre outras. Como ressalta (Gomes, L. F., & Pierangeli, J. H., 2011)., o Brasil possui um "modelo reativo" de produção legislativa penal, que responde a episódios midiáticos com leis de escopo limitado, desarticuladas entre si e com baixa eficácia a médio prazo.

Essa ausência de uma estrutura unificada se agrava com a sobreposição normativa e a existência de zonas cinzentas de competência entre esferas federal e estadual. A Polícia Federal possui atribuição constitucional para investigar crimes transnacionais ou que envolvam bens, serviços e interesses da União (Constituição Federal, art. 144, §1º, inciso I), mas a tipificação e o processamento de muitos crimes digitais ocorrem na justiça estadual, gerando disputas de competência e entraves operacionais. Em diversos casos, há duplicidade de investigações ou falhas na comunicação entre órgãos que, em tese,

deveriam atuar de forma coordenada (Dutra, L., 2023). Essa desarticulação compromete a agilidade da resposta estatal e permite que condutas sofisticadas escapem ao controle penal.

No plano processual, a fragmentação se reflete na dificuldade de padronização das diligências digitais. O Código de Processo Penal brasileiro (Decreto-Lei n.º 3.689/1941), embora reformado em pontos específicos, ainda opera sob uma lógica analógica e pouco técnica. Faltam previsões expressas sobre preservação de dados digitais, interceptações telemáticas com criptografia, e perícias baseadas em hashcodes. Além disso, não há normas consolidadas sobre a cadeia de custódia digital, o que torna as provas eletrônicas vulneráveis a contestações sobre autenticidade e integridade, principalmente em ações penais de alto impacto (Muneymne, 2025)

A ausência de um sistema unificado também repercute negativamente na formação dos operadores jurídicos. Em Portugal, a concentração normativa facilita a criação de programas de formação específicos e constantes, voltados à aplicação prática dos instrumentos legais vigentes. No Brasil, a diversidade de normas, muitas vezes contraditórias entre si, torna o processo de capacitação mais complexo, com foco excessivo em doutrina interpretativa e menor consistência técnico-operacional. Isso gera lacunas na atuação da magistratura, do Ministério Público e da advocacia, que precisam se adaptar a um arcabouço legal instável, constantemente reformado e por vezes inaplicável à realidade digital concreta (Szabó, 2023)

Do ponto de vista da cooperação internacional, o sistema unificado português facilita o cumprimento das obrigações assumidas no âmbito da Convenção de Budapeste, permitindo respostas jurídicas rápidas, coordenação institucional e integração com mecanismos de troca de dados em tempo real, como o e-Evidence. No Brasil, a ausência de adesão à Convenção e a inexistência de uma estrutura legislativa única dificultam a interlocução com outros países, principalmente no que diz respeito à obtenção de provas localizadas no exterior, à responsabilização de plataformas digitais e à recuperação de ativos oriundos de fraudes cibernéticas internacionais (Fonseca & Gennarini, 2022)..

Outro aspecto relevante é o impacto simbólico de um sistema penal fragmentado. A dispersão normativa transmite à sociedade a ideia de que o Estado está sempre correndo atrás da criminalidade digital, em vez de antecipá-la. Isso reduz a eficácia preventiva da

legislação penal e afeta a credibilidade das instituições encarregadas da repressão penal. Em contraposição, o sistema unificado português, mesmo com suas limitações, reforça a imagem de um Estado estruturado, que compreende o ciberespaço como um novo território jurídico a ser governado por normas claras, acessíveis e operacionais.

Em síntese, a comparação entre o sistema unificado português e o sistema fragmentado brasileiro evidencia a influência estrutural que o modelo legislativo exerce sobre a capacidade do Estado de enfrentar o cibercrime. A unificação normativa não é garantia de sucesso, mas oferece um terreno mais fértil para a construção de uma política criminal coerente, preventiva e eficaz. Já a fragmentação compromete a articulação institucional, a previsibilidade jurídica e a formação técnica dos agentes públicos, abrindo espaço para a impunidade e para a proliferação de condutas ilícitas cada vez mais complexas.

Diante desse cenário, impõe-se a necessidade de uma reforma estrutural do ordenamento jurídico brasileiro, com a criação de um Código Penal Digital ou, ao menos, de um capítulo específico no Código Penal voltado aos crimes informáticos. Essa iniciativa deve ser acompanhada da revisão do Código de Processo Penal, com a inserção de dispositivos sobre diligências eletrônicas, perícias digitais, cooperação internacional em tempo real e proteção das garantias fundamentais no ambiente virtual. Só assim o Brasil poderá superar as limitações impostas por seu atual sistema fragmentado e construir uma resposta penal à altura dos desafios contemporâneos do cibercrime.

2.6 Efetividade Processual: Meios de Prova, Investigação e Responsabilização Penal

A efetividade do processo penal no combate ao cibercrime depende da articulação entre normas jurídicas, infraestrutura técnico-operacional e capacitação dos operadores do sistema de justiça. No cenário digital, essa dinâmica se torna ainda mais complexa, considerando a volatilidade das provas, a transnacionalidade das condutas criminosas e a sofisticação tecnológica dos agentes delitivos. A investigação e a responsabilização penal exigem um modelo processual que seja não apenas legalmente eficaz, mas tecnicamente compatível com as características do ciberespaço. A análise comparativa entre Portugal e Brasil revela avanços, lacunas e desafios concretos enfrentados por ambos os países na busca por um sistema processual penal adaptado à realidade cibernética.

No âmbito da colheita da prova, uma das principais questões enfrentadas nos dois países diz respeito à preservação e autenticidade dos elementos digitais. A prova eletrônica, por sua natureza volátil e mutável, exige procedimentos de captura e armazenamento altamente técnicos, sob pena de perda de confiabilidade. Em Portugal, a Lei do Cibercrime (Lei n.º 109/2009) estabelece, em conformidade com a Convenção de Budapeste, regras claras sobre a preservação imediata de dados informáticos, tanto de conteúdo quanto de tráfego, permitindo inclusive ordens judiciais de conservação por 90 dias, prorrogáveis (art. 12.º). Essa previsão confere segurança jurídica à atuação dos investigadores e estabelece um protocolo uniforme de preservação, respeitando o princípio da legalidade e os direitos fundamentais (Verdelho, Bravo & Rocha, 2003).

No Brasil, embora o Marco Civil da Internet (Lei n.º 12.965/2014) tenha trazido dispositivos semelhantes nos artigos 13 a 15, a aplicação prática desses comandos enfrenta obstáculos operacionais. A ausência de regulamentação técnica detalhada, aliada à falta de padronização nos procedimentos das polícias e do Ministério Público, leva à produção de provas digitais sem observância adequada à cadeia de custódia. Essa situação tem motivado decisões judiciais que desconsideram provas relevantes por ausência de critérios mínimos de preservação, contrariando os objetivos do processo penal (Machado, 2022). A insegurança jurídica que resulta dessa fragilidade compromete diretamente a responsabilização penal de infratores cibernéticos, sobretudo em casos complexos que envolvem múltiplos dispositivos, redes anônimas e ferramentas de encriptação.

A cadeia de custódia digital é, portanto, um dos pontos mais sensíveis da efetividade processual em matéria de cibercrime. Em Portugal, a jurisprudência tem reconhecido a importância da rastreabilidade absoluta da prova eletrônica, exigindo a documentação de todas as ações periciais realizadas, inclusive os comandos utilizados e os logs de acesso aos sistemas periciados. A dificuldade na aplicação do artigo 158-A do CPP às provas digitais é discutida por Muneymne (2025). Essa exigência impõe uma cultura de responsabilidade técnica aos peritos e fortalece a confiabilidade das evidências apresentadas em juízo. No Brasil, embora o artigo 158-A do Código de Processo Penal tenha sido recentemente introduzido para disciplinar a cadeia de custódia, ainda há enorme dificuldade em aplicá-lo às provas digitais, principalmente em razão da falta de capacitação das equipes técnicas e da inexistência de protocolos nacionais unificados. A implementação da cadeia de custódia digital no Brasil é incipiente (Machado, 2022).

Outro ponto crítico é a obtenção judicial de provas junto a provedores de internet e plataformas digitais, muitos dos quais situados fora da jurisdição nacional. Portugal, como signatário da Convenção de Budapeste e membro da União Europeia, integra sistemas de cooperação como o Eurojust, o e-Evidence e a Rede Judiciária Europeia, que possibilitam trocas rápidas e seguras de dados com outros países. Essa inserção permite ao Ministério Público português solicitar informações diretamente a empresas com sede na Europa, com base em mecanismos harmonizados de assistência mútua. A cooperação internacional em matéria de cibercrime é destacada no relatório de atividades do membro nacional de Portugal na Eurojust (2022). O Brasil, por sua vez, encontra-se à margem desses instrumentos multilaterais, o que dificulta a obtenção de dados essenciais em tempo útil. A dependência de cartas rogatórias e acordos bilaterais resulta em morosidade e, muitas vezes, na inutilização das provas por decurso de prazo, especialmente em investigações que exigem resposta imediata. A morosidade na obtenção de provas digitais em investigações internacionais é um desafio enfrentado pelo Brasil (Fonseca & Gennarini, 2022).

A responsabilização penal dos autores de crimes digitais também esbarra em desafios estruturais. Em muitos casos, a identificação do autor é dificultada pelo uso de redes anônimas, VPNs, criptografia e perfis falsos. Para contornar essa dificuldade, é necessário O uso intensivo de técnicas de perícia digital, análise forense de dispositivos e inteligência artificial aplicada à mineração de dados. Em Portugal, a Polícia Judiciária conta com a Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T), que dispõe de laboratórios próprios de perícia digital e analistas especializados. Essa estrutura permite a realização de investigações com alto grau de sofisticação, o que, aliado a uma legislação clara, possibilita o oferecimento de denúncias com robustez probatória. A utilização de inteligência artificial nas perícias da Polícia Judiciária é destacada por Calé (2024).

No Brasil, a realidade é mais desigual. Embora a Polícia Federal conte com o Serviço de Repressão a Crimes Cibernéticos (SRCC), muitos estados não possuem delegacias especializadas ou estrutura mínima para análise forense digital. A consequência é a formação de investigações superficiais, baseadas em print screens, depoimentos frágeis ou cópias não periciadas de conversas eletrônicas. Isso compromete seriamente a responsabilização penal, permitindo que crimes como pornografia infantil, estelionato

eletrônico e extorsão sexual virtual sejam arquivados por ausência de justa causa ou convertidos em penas mínimas por falta de provas robustas. A jurisprudência reconhece que o armazenamento automático de imagens não configura crime sem prova inequívoca de dolo (TJDFT, 2020).

Além da coleta e preservação das provas, a efetividade do processo penal também depende da qualidade do juízo de admissibilidade e da correta valoração da prova digital. Em Portugal, os tribunais superiores têm afirmado com regularidade que a prova digital deve ser analisada com os mesmos critérios de qualquer outro meio probatório, mas com atenção especial à sua integridade e autenticidade. O Acórdão do Supremo Tribunal de Justiça, de 10 de maio de 2021 (Proc. n.º 92/19.0TELSB.L1.S1), estabeleceu parâmetros para a validade de e-mails como prova documental, exigindo a verificação da origem, integridade e contexto. No Brasil, embora haja avanços na jurisprudência, como o REsp 1.975.352/SP (STJ, 2022), que reconheceu a validade de prints desde que acompanhados de ata notarial, ainda há decisões conflitantes que ora aceitam, ora rejeitam provas digitais com base em critérios subjetivos, o que compromete a uniformidade da jurisprudência. A dificuldade na aplicação do artigo 158-A do CPP às provas digitais é discutida por (Muneymne, 2025)

Outro ponto crucial é o papel dos operadores do direito no manejo da prova digital. Uma alternativa sólida é o Aviso n.º 8/2024, emitido pelo Conselho Superior da Magistratura (CSM) e pelo Centro de Estudos Judiciários (CEJ), que detalha as ações de formação contínua para magistrados no biênio 2024-2025. Este documento destaca a inclusão de módulos sobre cibercriminalidade, segurança de redes e criptografia, evidenciando o compromisso das instituições em capacitar os operadores jurídicos para lidar com as complexidades do ciberespaço No Brasil, embora o CNJ tenha instituído programas de capacitação, sua implementação ainda é incipiente, e muitos juízes e promotores seguem aplicando a lógica do processo penal analógico a realidades digitais, o que gera decisões desconectadas da realidade tecnológica dos crimes julgados.

Adicionalmente, a ausência de especialização nas varas criminais e nos tribunais superiores afeta a efetividade da responsabilização penal. Em Portugal, os tribunais de comarca e os tribunais de relação contam com juízes especializados em crimes informáticos, o que acelera o trâmite processual e permite decisões mais técnicas (Portal Europeu da Justiça, s.d.). No Brasil, a Justiça ainda lida com a universalização de

competência, e o excesso de processos impede que magistrados se dediquem adequadamente aos crimes digitais, que exigem atenção técnica e análise aprofundada. Isso compromete a celeridade e a consistência das decisões, contribuindo para a sensação de impunidade e desestímulo à denúncia das vítimas (Legale, 2025).

Por fim, deve-se destacar que a efetividade processual em matéria de cibercrime depende também da adequação dos mecanismos de responsabilização penal a novas figuras típicas, como influenciadores digitais que incitam crimes, operadores de mercados ilegais virtuais, desenvolvedores de malware e administradores de redes criminosas descentralizadas. A identificação dessas figuras exige flexibilidade interpretativa e atualização constante da jurisprudência, além de técnicas de investigação que considerem a cadeia de comando em ambientes digitais, mesmo quando não há contato físico entre os envolvidos (Almeida, 2022; Ramalho, 2013).

Em suma, a efetividade processual no combate ao cibercrime depende de uma conjugação complexa de fatores: normas jurídicas adaptadas, provas tecnicamente válidas, operadores capacitados e cooperação internacional efetiva. Portugal, apesar das limitações orçamentárias, apresenta um sistema mais coeso, articulado e especializado. O Brasil, por sua vez, ainda enfrenta desafios estruturais graves, derivados da fragmentação normativa, da deficiência técnica e da ausência de especialização funcional. Superar esses obstáculos exige reformas institucionais, investimentos em capacitação e uma nova cultura processual penal que reconheça o ciberespaço como ambiente legítimo de persecução penal e tutela jurisdicional.

Capítulo 3 - Lacunas Legislativas e a Urgente Necessidade de Modernização no Combate ao Cibercrime no Brasil

A consolidação de um arcabouço normativo capaz de responder aos desafios impostos pelo cibercrime exige mais do que a simples adoção de leis pontuais. No contexto brasileiro, a legislação vigente revela uma defasagem significativa diante da complexidade técnica, fluidez e transnacionalidade das condutas delituosas praticadas no ambiente digital. Já em Portugal, embora exista uma maior harmonização com instrumentos internacionais, como a Convenção de Budapeste, ainda persistem lacunas normativas e operacionais que comprometem a efetividade da repressão e da prevenção.

Este capítulo examina com profundidade as lacunas estruturais e legislativas que limitam a eficácia do combate ao cibercrime, com destaque para os entraves normativos no Brasil e a necessidade de atualização constante frente às transformações tecnológicas. A análise a seguir contempla aspectos estruturais do ordenamento penal brasileiro e seus reflexos práticos, servindo de base para a compreensão crítica da ausência de sistematização jurídica no campo da criminalidade digital.

Aprofundando essa investigação, o capítulo seguinte será dedicado a um estudo empírico documental, no qual serão analisadas, comparativamente, as legislações do Brasil e de Portugal, com base em normas nacionais e tratados internacionais, em especial a Convenção de Budapeste.

3.1 A Ausência De Um Código Penal Digital No Brasil: Lacunas Normativas E Consequências Estruturais

O avanço exponencial das tecnologias digitais nas últimas duas décadas redefiniu o conceito de criminalidade e as formas de atuação delituosa. O ciberespaço, antes considerado um território marginal do Direito Penal, tornou-se palco privilegiado para crimes de alta complexidade, impacto transnacional e dificuldade probatória. Nesse novo cenário, a criminalidade se dissocia de fronteiras geográficas e assume formas altamente dinâmicas, o que impõe aos Estados nacionais a necessidade de revisar, adaptar e modernizar seus sistemas legislativos com urgência e profundidade. No entanto, o Brasil permanece com um arcabouço normativo desatualizado e fragmentado, ineficiente para conter a escalada dos crimes cibernéticos que afetam não apenas a segurança individual, mas também a integridade de sistemas governamentais, infraestruturas críticas, instituições financeiras e dados sensíveis da população (Silva, 2021).

A incapacidade do sistema jurídico brasileiro de acompanhar a velocidade das transformações digitais gerou um desequilíbrio evidente entre a sofisticação das práticas criminosas e os instrumentos legais disponíveis para reprimi-las. Crimes como invasão de sistemas, extorsão mediante ransomware, fraudes bancárias eletrônicas, clonagem de identidade digital, espionagem industrial, disseminação de desinformação automatizada e ataques de negação de serviço distribuída (DDoS) tornaram-se recorrentes, mas ainda carecem de previsão legal específica, sistemática e eficaz no ordenamento penal brasileiro (Neves, 2020). A dependência de interpretações extensivas ou analogias jurídicas, em vez

de normas claras e adaptadas à realidade digital, contribui para decisões judiciais dissonantes, insegurança jurídica e baixa taxa de responsabilização penal.

A gravidade desse problema é intensificada quando se observa a ausência de um Código Penal Digital no Brasil. O Código Penal de 1940, concebido em um período anterior à era da informação, ainda constitui a espinha dorsal do sistema penal brasileiro. Embora tenha sofrido alterações pontuais ao longo do tempo, como a introdução de crimes relacionados a dispositivos informáticos pela Lei n.º 12.737/2012 (conhecida como Lei Carolina Dieckmann), e a regulação de aspectos civis da internet pelo Marco Civil da Internet (Lei n.º 12.965/2014), o país ainda não consolidou em um único diploma jurídico as condutas típicas, os procedimentos processuais e os regimes sancionatórios próprios da criminalidade digital. Essa ausência de sistematização representa não apenas uma lacuna legislativa, mas também uma omissão política e institucional frente a um fenômeno em crescimento exponencial (Ferreira & Lopes, 2021).

A comparação com o cenário europeu, e em especial com Portugal, evidencia ainda mais a defasagem brasileira. Portugal aprovou a Lei n.º 109/2009, que estabelece o regime jurídico aplicável à criminalidade informática e transpõe para o ordenamento interno a Convenção de Budapeste, principal tratado internacional sobre o combate ao cibercrime. Essa legislação oferece uma abordagem integrada e proativa, prevendo crimes como o acesso ilegítimo, a interceção de comunicações, a interferência em sistemas e dados, bem como a falsidade informática e a fraude digital. Além disso, estabelece medidas de cooperação jurídica internacional e preservação de provas digitais, possibilitando uma atuação coordenada e ágil entre os países signatários (Santos, 2022). O Brasil, por sua vez, ainda não aderiu à Convenção de Budapeste, o que restringe sua capacidade de cooperação transnacional e o coloca à margem dos esforços globais de enfrentamento ao cibercrime.

Além da deficiência legislativa, o país enfrenta severos entraves operacionais e estruturais. A ausência de regulamentação específica para procedimentos como a apreensão de dispositivos eletrônicos, a preservação e autenticação de provas digitais, a interceptação telemática e o compartilhamento internacional de dados compromete diretamente a efetividade das investigações criminais. Os agentes de persecução penal muitas vezes operam sem protocolos claros, utilizando ferramentas técnicas inadequadas ou ineficientes, o que resulta em nulidades processuais, contestações quanto à cadeia de

custódia e arquivamentos por ausência de provas robustas (Martins, 2021). Essa situação é agravada pela falta de formação especializada dos operadores do Direito, que se veem obrigados a interpretar conceitos e lidar com tecnologias complexas sem a capacitação técnica necessária.

No campo da persecução penal, a ausência de um sistema jurídico atualizado também compromete a segurança jurídica das decisões judiciais. Como não há tipificações claras e atualizadas sobre a maioria das condutas cibernéticas, os magistrados se veem diante de um duplo desafio: aplicar normas concebidas para o mundo analógico a crimes altamente tecnológicos, e fundamentar suas decisões com base em interpretações extensivas que muitas vezes carecem de respaldo doutrinário e jurisprudencial sólido. Tal cenário contribui para a insegurança jurídica, favorecendo a impunidade ou a fragilização das garantias fundamentais, gerando precedentes contraditórios e instabilidade institucional.

A ausência de normas específicas também afeta profundamente a responsabilização penal das grandes corporações tecnológicas. Empresas responsáveis por plataformas digitais, provedores de internet, serviços de armazenamento em nuvem e redes sociais frequentemente resistem à entrega de informações sensíveis ou à cooperação com investigações criminais, amparadas na falta de legislação clara que as obrigue à colaboração. A inexistência de sanções objetivas e proporcionais a essas entidades por omissão ou resistência agrava ainda mais o déficit normativo e prejudica a efetividade do sistema de justiça criminal. Em Portugal, a legislação já prevê obrigações específicas às entidades detentoras de dados, com previsão de medidas coercitivas e multas em caso de descumprimento, o que tem proporcionado maior colaboração e celeridade nas investigações (Ferreira & Lopes, 2021).

Adicionalmente, a inexistência de políticas públicas coordenadas e de um plano nacional de enfrentamento ao cibercrime compromete a capacidade reativa e preventiva do Estado brasileiro. A proteção de dados, a segurança cibernética e a criminalidade digital são tratadas de forma dispersa por diferentes órgãos e esferas de governo, sem diretrizes unificadas ou estratégia nacional consolidada. Esse descompasso institucional gera sobreposição de funções, duplicidade de esforços e ineficiência sistêmica, além de dificultar o monitoramento e a avaliação das políticas públicas implementadas. Países como a França, a Estônia e a Alemanha já contam com estratégias nacionais de cibersegurança integradas ao seu sistema penal, o que demonstra o caminho necessário

para o Brasil alcançar maior efetividade e racionalidade no enfrentamento aos crimes cibernéticos.

3.2 A Defasagem da Legislação Brasileira em Relação à Realidade Digital

A defasagem da legislação penal brasileira diante da realidade digital representa um dos maiores obstáculos à repressão eficaz dos crimes cibernéticos no país. Embora o avanço da tecnologia tenha transformado profundamente a dinâmica da criminalidade, o ordenamento jurídico nacional não acompanhou com igual velocidade essas mudanças, resultando em um vácuo normativo que favorece a impunidade, a insegurança jurídica e a ineficiência do sistema de justiça criminal. A lacuna existente entre a sofisticação das práticas criminosas digitais e os instrumentos legais disponíveis para enfrentá-las é cada vez mais evidente, especialmente quando se compara o modelo brasileiro a experiências mais consolidadas, como a portuguesa.

O Código Penal brasileiro, datado de 1940, foi concebido em um contexto histórico e social totalmente distinto do atual. As condutas típicas previstas na época não contemplavam a possibilidade de delitos praticados por meio de redes digitais, em ambientes virtuais ou com a intermediação de algoritmos automatizados. Desde então, embora tenha havido reformas pontuais com o objetivo de incorporar novas tipificações penais, essas atualizações foram insuficientes para configurar um regime normativo robusto e sistematizado voltado ao cibercrime (Santana, 2021). Leis como a n.º 12.737/2012 (Lei Carolina Dieckmann), a n.º 12.965/2014 (Marco Civil da Internet) e a n.º 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) introduziram aspectos importantes, mas não solucionaram o problema de fundo: a ausência de um corpo legislativo unificado, moderno e especializado em criminalidade digital.

O Brasil ainda trata os crimes cibernéticos como exceções normativas, distribuídas entre dispositivos esparsos, o que compromete a clareza, a coerência e a efetividade das normas penais. Essa fragmentação legislativa dificulta a atuação dos operadores do Direito, prejudica a uniformidade jurisprudencial e fragiliza a resposta penal diante de condutas altamente especializadas, como ataques de ransomware, fraudes com uso de engenharia social, falsificação de identidades digitais e manipulação de dados sensíveis em larga escala. Além disso, a ausência de tipificações penais específicas obriga o Ministério Público e a magistratura a recorrerem a interpretações extensivas e analogias, o que,

embora necessário, enfraquece a segurança jurídica e gera decisões contraditórias nos tribunais (Silva, 2021).

Outro ponto de destaque é a falta de integração entre a legislação penal e a legislação processual no contexto dos delitos digitais. Mesmo quando a conduta criminosa encontra correspondência no tipo penal, a aplicação das normas processuais tradicionais revela-se inadequada para os métodos de investigação e instrução necessários ao cibercrime. O Código de Processo Penal, criado em 1941, não foi originalmente concebido para lidar com provas eletrônicas, cadeias de custódia digitais ou medidas coercitivas envolvendo plataformas transnacionais de tecnologia. A ausência de regulamentação específica sobre esses temas compromete não apenas a produção probatória, mas também o respeito aos direitos fundamentais em procedimentos que envolvem coleta de dados pessoais, interceptação de comunicações digitais e acesso remoto a dispositivos eletrônicos (Martins, 2021).

A experiência portuguesa oferece um contraste elucidativo. Portugal, desde a década de 2000, tem implementado reformas legislativas estruturadas no sentido de consolidar um regime jurídico penal específico para a criminalidade informática. A promulgação da Lei n.º 109/2009, que transpôs a Convenção de Budapeste para o ordenamento interno, representou um marco no enfrentamento do cibercrime. Essa legislação contempla, em um único diploma, tipos penais, procedimentos processuais e mecanismos de cooperação internacional voltados exclusivamente para os crimes cometidos em ambiente digital. A sistematização normativa confere segurança jurídica, previsibilidade e eficiência à atuação das autoridades públicas, além de facilitar a formação técnica dos operadores jurídicos (Santos, 2022).

A lei portuguesa prevê, por exemplo, a criminalização do acesso ilegítimo a sistemas informáticos (art. 3.º), da interceção de comunicações (art. 4.º), da interferência em sistemas e dados (arts. 5.º e 6.º), da falsidade informática (art. 7.º) e da fraude informática (art. 8.º). Além disso, regula a responsabilidade penal das pessoas coletivas (art. 13.º), a competência internacional (art. 14.º) e os procedimentos de cooperação transfronteiriça. Essa abordagem integrada permite que Portugal atue de forma coordenada com outros países, compartilhe provas com celeridade e adote medidas investigativas compatíveis com a realidade do ciberespaço, como a conservação rápida de dados (art. 12.º) e o acesso a sistemas armazenados de forma remota (Ferreira & Lopes, 2021).

O Brasil, por outro lado, não dispõe de mecanismos semelhantes consolidados. Os dispositivos existentes são insuficientes para abarcar toda a complexidade da criminalidade digital e não formam um corpo normativo coerente. A Lei n.º 12.965/2014, embora importante para estabelecer princípios e garantias no uso da internet, tem natureza essencialmente civil e principiológica, não se destinando à repressão penal. Já a LGPD, de cunho predominantemente regulatório, concentra-se na proteção de dados pessoais sob a ótica administrativa e consumerista, sem criar novos tipos penais ou prever mecanismos de persecução penal específicos. A Lei Carolina Dieckmann, por sua vez, apesar de ter tipificado condutas como a invasão de dispositivo informático, o fez de maneira limitada, com redação genérica e penalidades relativamente brandas (Ferreira da Silva Ramalho, 2024).

A inexistência de um Código Penal Digital ou de uma seção específica e estruturada no Código Penal vigente para tratar dos crimes informáticos prejudica não apenas a repressão, mas também a prevenção e a conscientização social sobre os riscos do ciberespaço. A legislação penal desempenha função simbólica e educativa na sociedade, e a ausência de normas claras sobre condutas cibernéticas colabora para a banalização de práticas ilícitas na internet, como golpes financeiros, fraudes com documentos eletrônicos, crimes contra a honra em redes sociais e distribuição de conteúdo sensível sem consentimento. Tal lacuna desestimula a denúncia por parte das vítimas, gera descrédito no sistema de justiça e dificulta campanhas institucionais de prevenção (Bechara, 2021).

A proposta de criação de um Código Penal Digital no Brasil vem sendo debatida por juristas, legisladores e especialistas em segurança da informação, mas ainda não avançou de forma concreta no Congresso Nacional. Tal instrumento normativo deveria consolidar, de forma sistemática, todas as infrações penais praticadas em ambiente digital, bem como estabelecer critérios objetivos para sua aplicação, definição de penas proporcionais, procedimentos de investigação e diretrizes de cooperação internacional. Um código dessa natureza poderia seguir o modelo europeu, inspirando-se em legislações como a portuguesa, a alemã e a francesa, que já adotam normas integradas e específicas para enfrentar a criminalidade cibernética de maneira proativa (Ferreira da Silva Ramalho, 2024).

Além da estrutura legal, a implementação de uma política pública nacional de segurança digital é igualmente imprescindível. A criação de um marco legal não será suficiente se não vier acompanhada de medidas estruturantes, como a capacitação permanente de juízes, promotores, delegados e peritos forenses; o investimento em tecnologia de ponta para investigação criminal; a criação de delegacias e varas especializadas em cibercrime; e o desenvolvimento de uma cultura institucional orientada à atuação em ambiente virtual. Esses elementos são indispensáveis para que a legislação produza efeitos reais e contribua para a efetiva tutela penal dos bens jurídicos ameaçados no ciberespaço.

Em síntese, a defasagem da legislação brasileira em relação à realidade digital é um problema estrutural, multifacetado e urgente. A ausência de um corpo normativo coeso, moderno e específico compromete a repressão penal, prejudica a atuação dos operadores do Direito, reduz a segurança jurídica e favorece a impunidade. O contraste com Portugal e outros países europeus demonstra que é possível, por meio de reformas legislativas estruturadas, construir um modelo jurídico eficaz e adaptado à complexidade da era digital. O Brasil precisa deixar de atuar de forma reativa e fragmentada, assumindo uma postura proativa na construção de um ordenamento penal à altura dos desafios do século XXI

3.3 O Impacto da Falta de Normatização na Investigação Criminal

A eficácia da investigação criminal em matéria de cibercrime depende, de forma incontornável, da existência de um arcabouço legal sólido, claro e tecnicamente ajustado à realidade digital. No entanto, no Brasil, a ausência de normatização adequada para lidar com os desafios específicos das infraestruturas tecnológicas, das plataformas virtuais e dos dispositivos digitais tem comprometido a qualidade, a celeridade e a legitimidade das investigações. Essa lacuna legislativa fragiliza a obtenção de provas, prejudica a rastreabilidade dos atos ilícitos e contribui para a impunidade de condutas que, embora sofisticadas, não encontram respaldo normativo processual compatível com sua complexidade (Martins, 2021).

A investigação de crimes digitais requer protocolos precisos para coleta, preservação, análise e validação de provas eletrônicas. Sem regras claras sobre como capturar dados de logs, endereços IP, conversas criptografadas ou conteúdos armazenados em nuvem, os agentes públicos ficam à mercê de interpretações subjetivas, improvisações operacionais

e decisões contraditórias do Poder Judiciário. Em muitos casos, a ausência de parâmetros normativos leva à invalidação de provas por violação à cadeia de custódia digital, o que implica diretamente na absolvição de réus que, embora culpados, não podem ser responsabilizados juridicamente diante de falhas processuais insanáveis (Bechara, 2020).

Diferentemente de investigações tradicionais, que lidam com objetos físicos, testemunhos presenciais e perícias materiais, os crimes cibernéticos exigem o domínio de técnicas digitais e a adoção de medidas ágeis para impedir a perda irreversível de dados. O tempo, nesse contexto, é um fator determinante. Dados trafegam em milésimos de segundo, são apagados ou criptografados com facilidade, e as evidências podem estar armazenadas em servidores localizados em múltiplos países. A ausência de normatização sobre a preservação emergencial de dados e os procedimentos de congelamento de informações sensíveis compromete a integridade do processo investigativo no Brasil (Silva, 2021).

O Marco Civil da Internet (Lei n.º 12.965/2014), embora represente um avanço no campo das garantias digitais, não oferece diretrizes detalhadas sobre como as autoridades devem agir para capturar, manter e acessar dados eletrônicos de maneira juridicamente válida. A lei estabelece, em seus artigos 13 a 15, prazos para guarda de registros de conexão e acesso a aplicações, mas não regulamenta, por exemplo, os formatos aceitos para validação probatória, os parâmetros de integridade técnica ou a atuação dos provedores em casos de requisição judicial urgente. A Lei Geral de Proteção de Dados (Lei n.º 13.709/2018), por sua vez, prioriza a tutela do titular de dados, mas pouco se debruça sobre a interface entre privacidade e persecução penal, o que resulta em conflitos frequentes entre direitos fundamentais e interesse público na investigação (Ramalho & Almeida, 2024).

A ausência de legislação específica sobre apreensão de dispositivos eletrônicos é igualmente problemática. Não há regulamentação nacional sobre como devem ser efetuadas buscas e apreensões de computadores, smartphones e outros dispositivos de armazenamento digital, nem sobre os requisitos técnicos mínimos para a sua análise forense. Em consequência, é comum que provas digitais sejam extraídas sem perícia adequada, sem duplicação fiel via hashcode, ou até mesmo com acesso irrestrito e não documentado por agentes públicos, comprometendo a validade da prova e violando princípios como o devido processo legal e a inviolabilidade da intimidade (Carvalho, 2023).

Portugal, por outro lado, apresenta uma realidade significativamente mais estruturada. A Lei n.º 109/2009, que regula a criminalidade informática, inclui capítulos específicos sobre medidas processuais e instrumentos de obtenção de prova digital. O artigo 12.º, por exemplo, trata da conservação rápida de dados, autorizando as autoridades a requisitarem que determinados elementos informáticos sejam preservados por prazos iniciais de 90 dias. O artigo 15.º trata do acesso a sistemas informáticos, estabelecendo salvaguardas e limites para evitar abusos. Essa normatização confere previsibilidade, segurança jurídica e eficiência ao trabalho policial e ministerial, permitindo que os tribunais portugueses validem a prova obtida com base em critérios técnicos padronizados (Ferreira & Lopes, 2021).

Além da legislação especializada, Portugal conta com órgãos de investigação dotados de estrutura técnico-científica, como a Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T), vinculada à Polícia Judiciária. Essa unidade atua com base em protocolos próprios de coleta, análise e conservação de evidências digitais, alinhados aos padrões europeus estabelecidos pela Europol e pela Convenção de Budapeste. A existência de tais procedimentos operacionais padronizados permite maior confiabilidade nas provas obtidas, reduzindo nulidades processuais e fortalecendo a responsabilização penal (Santos, 2022).

No Brasil, a situação é marcadamente desigual. Enquanto a Polícia Federal possui uma divisão especializada em crimes cibernéticos, com capacidade técnica reconhecida, as polícias civis dos estados operam, em sua maioria, sem departamentos voltados à investigação digital. A realidade é agravada pela carência de equipamentos, ausência de peritos em tecnologia da informação e rotatividade de agentes sem formação específica. Em alguns estados, investigações de crimes complexos, como estelionato eletrônico e pornografia infantil online, são conduzidas por delegacias distritais sem qualquer preparo técnico para lidar com material digital sensível, resultando em investigações precárias, inconclusivas ou passíveis de nulidade absoluta (Almeida & Castro, 2023).

Outro ponto crítico é a atuação do Poder Judiciário na fase de investigação preliminar. Em razão da falta de legislação clara, muitos juízes divergem sobre a legalidade de medidas como acesso remoto a arquivos, bloqueio de contas em plataformas digitais, geolocalização de dispositivos e interceptação de comunicações em aplicativos criptografados. Algumas decisões autorizam o uso de softwares forenses invasivos com

base em interpretações extensivas da legislação analógica; outras, ao contrário, consideram tais medidas inconstitucionais por ausência de previsão legal específica. Essa falta de uniformidade prejudica o planejamento das investigações, gera insegurança para os agentes públicos e estimula recursos protelatórios por parte das defesas (Martins, 2022).

A problemática se agrava quando há necessidade de cooperação internacional. No ciberespaço, é comum que os dados relevantes estejam armazenados em servidores de empresas transnacionais, especialmente nos Estados Unidos. Como o Brasil ainda não aderiu à Convenção de Budapeste, os pedidos de cooperação internacional enfrentam burocracias prolongadas e, muitas vezes, não são respondidos a tempo de garantir a efetividade da investigação. A inexistência de um acordo direto com empresas como Google, Meta ou Apple dificulta o acesso a dados essenciais para o esclarecimento de crimes, como registros de IP, históricos de login, conteúdo de mensagens e metadados. Portugal, por sua vez, integra plenamente a estrutura da Convenção de Budapeste e da União Europeia, o que lhe confere acesso facilitado a informações cruciais em investigações transnacionais (Neves, 2020).

A ausência de normatização também tem implicações no campo das garantias fundamentais. Em nome da repressão criminal, é frequente que agentes públicos, diante da urgência e da ausência de regras claras, acabem por violar direitos fundamentais como a privacidade, a inviolabilidade das comunicações e a presunção de inocência. A inexistência de protocolos normativos deixa margem para abusos, como o acesso indiscriminado a arquivos pessoais sem delimitação temporal ou material, e a divulgação pública de dados obtidos irregularmente. Em uma democracia, a efetividade da investigação não pode se dar em detrimento das garantias processuais, razão pela qual se exige legislação equilibrada, precisa e tecnicamente viável (Bechara, 2021)

3.4 A Falta de Cooperação Internacional e a Não Adesão à Convenção de Budapeste

A cooperação internacional constitui um dos pilares fundamentais para o enfrentamento eficaz dos crimes cibernéticos na contemporaneidade. Em um ambiente digital caracterizado pela transnacionalidade das condutas, pela descentralização dos dados e pela velocidade das ações ilícitas, a atuação isolada dos Estados nacionais revela-se não

apenas ineficiente, mas estruturalmente inviável. A criminalidade cibernética não conhece fronteiras, e suas manifestações mais sofisticadas envolvem agentes, servidores, infraestruturas e ativos localizados em diferentes jurisdições. Nesse contexto, a adesão a instrumentos multilaterais que promovam a harmonização legislativa e a integração operacional dos sistemas de justiça tornou-se uma exigência incontornável para qualquer país que pretenda responder de forma eficaz aos desafios do ciberespaço. O Brasil, ao permanecer fora da Convenção de Budapeste sobre o Cibercrime, compromete sua capacidade de atuação internacional, fragiliza sua soberania digital e limita o alcance das investigações criminais transfronteiriças, perpetuando uma condição de vulnerabilidade jurídica no plano global (Corrêa & Monteiro Neto, 2022).

A Convenção de Budapeste, formalmente denominada Convenção sobre o Cibercrime do Conselho da Europa, é o mais relevante instrumento jurídico internacional no campo do combate aos crimes informáticos. Desde sua adoção, em 2001, o tratado tornou-se referência normativa global, sendo subscrito por países europeus, americanos, asiáticos e africanos. A Convenção estabelece normas de direito material, direito processual e mecanismos de cooperação internacional voltados à criminalidade informática, incorporando uma visão integrada e moderna sobre a persecução penal em ambiente digital. Seu conteúdo contempla a tipificação de condutas como acesso não autorizado a sistemas, interceptação ilícita de comunicações, interferência em dados, falsidade e fraude informáticas, além de estabelecer procedimentos específicos para a preservação e coleta de provas eletrônicas, incluindo dados de tráfego e conteúdos armazenados remotamente (Conselho da Europa, 2001).

Portugal aderiu à Convenção de Budapeste desde o início de sua vigência, incorporando seus dispositivos ao ordenamento jurídico interno por meio da Lei n.º 109/2009. A legislação portuguesa passou a contar com um sistema jurídico plenamente compatível com os padrões internacionais de repressão ao cibercrime, o que permitiu ao país integrar redes de cooperação como a Eurojust, a Rede Judiciária Europeia e o e-Evidence, facilitando o intercâmbio de informações com outros países signatários. Essa integração fortaleceu a capacidade de investigação e atuação das autoridades portuguesas, sobretudo em casos que envolvem múltiplas jurisdições, empresas transnacionais ou plataformas sediadas fora do território nacional. Com isso, Portugal posicionou-se como parceiro confiável no combate ao cibercrime, beneficiando-se de acordos bilaterais e multilaterais

que possibilitam respostas ágeis, seguras e juridicamente sustentáveis (Ferreira & Lopes, 2021).

O Brasil, por sua vez, mantém-se em condição de não signatário da Convenção, o que representa um retrocesso estratégico diante da crescente sofisticação da criminalidade digital e da necessidade de articulação global para combatê-la. A não adesão implica uma série de prejuízos objetivos e subjetivos. No plano jurídico, significa que o país não está vinculado aos compromissos internacionais de harmonização legislativa, dificultando o reconhecimento recíproco de medidas processuais, a validação de provas obtidas no exterior e a execução de ordens judiciais oriundas de outros países. No plano operacional, a ausência de adesão restringe o acesso do Brasil a canais diretos de cooperação, obrigando-o a recorrer a instrumentos mais lentos, como as cartas rogatórias ou os pedidos de assistência jurídica mútua, muitas vezes ineficazes diante da volatilidade das provas digitais (Ramalho & Almeida, 2024).

A escolha por não integrar a Convenção de Budapeste coloca o Brasil em posição de isolamento no cenário internacional, gerando desconfiança entre as autoridades estrangeiras quanto à capacidade do país de colaborar de forma segura e eficaz nas investigações transnacionais. Esse isolamento compromete o fluxo de informações essenciais para a identificação e responsabilização de criminosos que atuam globalmente, como hackers, operadores de ransomware, agentes de espionagem cibernética e responsáveis por fraudes eletrônicas de larga escala. Em crimes como phishing internacional, sequestro de dados de empresas transnacionais ou disseminação de conteúdos ilegais por meio de redes estrangeiras, a ausência de cooperação automática resulta em perda de provas, paralisação das investigações e, muitas vezes, impunidade absoluta (Martins, 2022).

Um dos aspectos mais críticos da não adesão é a dificuldade em obter dados de provedores sediados no exterior, especialmente nos Estados Unidos, onde se concentram grandes plataformas digitais como Google, Meta, Apple, Microsoft e Amazon. Essas empresas, amparadas pela legislação norte-americana e por seus próprios termos de uso, não são obrigadas a responder diretamente às autoridades brasileiras, salvo quando há previsão legal compatível com os instrumentos de cooperação internacional em vigor. Como o Brasil não é signatário da Convenção, tampouco possui acordos bilaterais específicos com todas essas empresas, a obtenção de dados estratégicos, como registros de IP, mensagens

criptografadas, metadados de comunicação ou localização de dispositivos, torna-se extremamente morosa e incerta. Portugal, ao contrário, usufrui de canais preferenciais de requisição e conta com interlocutores institucionais estabelecidos, o que confere maior agilidade e efetividade às medidas investigativas (Santos, 2022).

A resistência brasileira em aderir à Convenção de Budapeste tem sido justificada por argumentos relacionados à soberania nacional e à alegada assimetria de interesses entre os países signatários. Alguns setores argumentam que o tratado teria sido concebido por países europeus e poderia comprometer a autonomia jurídica de países em desenvolvimento. No entanto, essa justificativa tem se mostrado cada vez mais insustentável, sobretudo diante da realidade de que países latino-americanos como Argentina, Chile e Costa Rica já se tornaram signatários do tratado, reconhecendo sua importância estratégica para o fortalecimento da segurança digital. Além disso, o próprio Conselho da Europa mantém diálogo constante com países interessados em aderir, oferecendo margens de flexibilização e adaptações compatíveis com os sistemas jurídicos locais, o que enfraquece o argumento da ingerência internacional (Neves, 2020).

No plano interno, a ausência de adesão à Convenção reflete também uma falta de prioridade política em relação à segurança cibernética e à proteção da infraestrutura digital nacional. O Brasil tem investido de forma tímida na modernização de seus instrumentos jurídicos e na criação de mecanismos de resposta integrada a ameaças digitais. Embora existam iniciativas pontuais, como o Comitê Gestor da Internet e os centros de resposta a incidentes, essas estruturas carecem de articulação normativa internacional e de respaldo legal adequado para atuarem em casos de crimes transnacionais. Sem a adesão à Convenção de Budapeste, o país limita sua capacidade de resposta a ataques cibernéticos coordenados, o que fragiliza não apenas a atuação policial e judicial, mas a própria segurança nacional (Corrêa & Monteiro Neto, 2022).

A não adesão também compromete a credibilidade do Brasil em fóruns multilaterais voltados à governança digital e ao combate à criminalidade transfronteiriça. Em um cenário global cada vez mais voltado à cooperação, os países que optam pelo isolamento legislativo e operacional perdem protagonismo político, acesso a tecnologias avançadas de investigação e oportunidades de integração institucional. A adesão à Convenção de Budapeste não é apenas uma medida jurídica, mas uma decisão estratégica de inserção internacional e de fortalecimento da soberania digital por meio da cooperação.

É importante destacar que aderir à Convenção não significa abrir mão da independência normativa ou das garantias constitucionais. O tratado respeita os princípios fundamentais dos sistemas jurídicos nacionais, exigindo apenas que os países signatários adotem medidas compatíveis com a repressão efetiva dos crimes cibernéticos, sem comprometer seus modelos jurídicos internos. O Brasil pode aderir ao tratado com reservas específicas, desde que compatíveis com os objetivos do instrumento, garantindo, assim, sua adaptação sem prejuízo da ordem constitucional vigente.

Portanto, a permanência do Brasil fora da Convenção de Budapeste constitui uma lacuna estratégica de grande impacto na luta contra o cibercrime. Essa condição prejudica o país em múltiplos níveis: compromete a eficiência das investigações criminais, impede o acesso a provas digitais cruciais, reduz a capacidade de resposta a ameaças transnacionais e enfraquece sua posição geopolítica. A adesão à Convenção deve ser encarada não como concessão de soberania, mas como fortalecimento da capacidade estatal de proteger seus cidadãos, suas instituições e sua economia diante dos riscos do ciberespaço. A integração jurídica internacional é hoje uma necessidade funcional, não apenas uma opção diplomática, e o Brasil não pode mais se furtar a essa responsabilidade sem comprometer gravemente sua atuação penal na era digital.

3.5 Propostas de Reforma para uma Legislação Proativa e Preventiva

A ausência de uma legislação penal digital sistematizada, atualizada e voltada à complexidade do cibercrime no Brasil não apenas dificulta a repressão eficaz das condutas ilícitas, mas compromete, de forma estrutural, a capacidade preventiva do Estado diante da crescente sofisticação dos delitos cibernéticos. O combate à criminalidade digital não se resolve unicamente com medidas reativas, centradas na responsabilização penal após a ocorrência do crime. É imprescindível construir um modelo normativo proativo, que antecipe comportamentos de risco, fortaleça as instituições, promova a educação digital da população e estabeleça mecanismos de compliance e auditoria compatíveis com o dinamismo do ciberespaço. Diante disso, este subtítulo propõe um conjunto de reformas que visam superar as deficiências identificadas ao longo deste capítulo, oferecendo ao ordenamento jurídico brasileiro bases concretas para a construção de uma legislação verdadeiramente estratégica e preventiva no enfrentamento ao cibercrime.

O primeiro e mais urgente passo é a elaboração e aprovação de um código penal digital brasileiro, concebido como um diploma normativo autônomo, integrado e especializado, que reúna em um único corpo legal as infrações penais cometidas em ambiente digital. Tal código deve abranger não apenas a descrição das condutas típicas – como invasão de dispositivos informáticos, interceptação ilícita de comunicações, fraudes eletrônicas, disseminação de malware, ataques de negação de serviço, crimes contra a honra praticados na internet e exposição não autorizada de dados pessoais – mas também regulamentar as medidas processuais cabíveis, as competências institucionais e os procedimentos de cooperação nacional e internacional. Inspirado na experiência portuguesa com a Lei n.º 109/2009 e no modelo da União Europeia de harmonização legislativa, o código penal digital brasileiro deve ser estruturado com base em critérios técnicos, respeitando os princípios constitucionais, mas com plena adaptação à lógica transfronteiriça e descentralizada da internet (Portugal, 2009).

Essa codificação representa não apenas um avanço legislativo, mas uma sinalização clara de prioridade institucional no combate ao cibercrime. Ao reunir os diversos tipos penais hoje dispersos em leis esparsas, o novo código conferirá clareza, segurança jurídica e previsibilidade à atuação dos operadores do Direito. Além disso, possibilitará a elaboração de políticas públicas coerentes e a construção de indicadores mais precisos sobre a criminalidade digital, contribuindo para o planejamento estratégico das ações repressivas e preventivas. A codificação também permitirá a atualização periódica das normas, facilitando a inclusão de novas condutas típicas à medida que surgem avanços tecnológicos relevantes, como os crimes envolvendo inteligência artificial generativa, manipulação algorítmica e ambientes de realidade aumentada.

Paralelamente à codificação penal, é imprescindível uma reforma no Código de Processo Penal que contemple as especificidades da persecução penal em ambiente digital. O atual CPP, datado de 1941, foi concebido sob a lógica de um processo penal tradicional, baseado em provas físicas, atos presenciais e procedimentos cartoriais. Essa lógica não se sustenta frente às particularidades do cibercrime, que exige velocidade, flexibilidade e domínio técnico. A reforma deve incluir dispositivos sobre a preservação de provas digitais, o uso de técnicas forenses compatíveis com os princípios da cadeia de custódia eletrônica, a regulamentação do acesso remoto a sistemas informáticos com autorização judicial, o uso de tecnologias de rastreamento de ativos digitais, a possibilidade de

produção antecipada de prova digital e a integração com bases de dados internacionais. O Brasil deve observar as melhores práticas internacionais nesse campo, incluindo as diretrizes da Convenção de Budapeste e os modelos legislativos adotados por Portugal, Alemanha e Estônia, países que já adaptaram seus procedimentos processuais às exigências da investigação cibernética (Portugal, 2009).

Outra medida essencial é a criação de unidades especializadas em cibercrime no âmbito do Ministério Público, do Poder Judiciário e das polícias judiciárias. A experiência portuguesa, com a atuação da Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T), demonstra que a especialização institucional é fator determinante para a efetividade da repressão penal. No Brasil, embora a Polícia Federal possua divisões específicas para crimes digitais, a grande maioria das polícias civis estaduais, promotorias de justiça e varas judiciais ainda opera sob lógica generalista, sem a capacitação técnica necessária para lidar com condutas de alta complexidade tecnológica. A criação de delegacias especializadas, núcleos de atuação integrada e varas com competência exclusiva para cibercrimes permitirá maior celeridade processual, maior segurança na análise da prova técnica e maior confiabilidade na responsabilização penal (UNC3T, 2024).

Essas estruturas devem ser acompanhadas de programas permanentes de formação técnica e capacitação jurídica, voltados para juízes, promotores, defensores públicos, advogados, policiais e peritos. A formação deve abranger conhecimentos em segurança da informação, criptografia, redes, inteligência artificial, engenharia reversa, análise de metadados, dark web, blockchain e legislação comparada. A complexidade do cibercrime exige operadores do Direito preparados não apenas para interpretar normas, mas para compreender o funcionamento dos meios pelos quais os crimes são cometidos, identificando padrões, vulnerabilidades e estratégias de prevenção. A formação continuada deve ser institucionalizada por meio de convênios com universidades, centros de pesquisa e organizações internacionais, como a Interpol e o Conselho da Europa.

Em paralelo à estruturação estatal, é indispensável o fortalecimento das medidas de compliance digital e corresponsabilização empresarial. Empresas que operam no Brasil, especialmente aquelas que atuam no setor de tecnologia, finanças, telecomunicações, saúde e educação, devem ser legalmente obrigadas a adotar sistemas de proteção de dados robustos, auditorias regulares de segurança cibernética e planos de contingência em caso

de incidentes. A legislação deve prever penalidades proporcionais à gravidade da falha e à extensão do dano causado, inclusive com sanções de natureza penal para casos de omissão deliberada ou negligência grave. A responsabilização das pessoas jurídicas por crimes cibernéticos, conforme previsto em legislações modernas como a portuguesa, é um passo necessário para consolidar um ecossistema digital mais seguro e ético (Portugal, 2009).

Além da responsabilização empresarial, é essencial que a legislação contemple instrumentos de estímulo à denúncia de condutas suspeitas, à colaboração premiada em crimes cibernéticos e à proteção de denunciantes. A implementação de canais seguros e sigilosos para denúncias anônimas, a previsão de acordos de não persecução penal para colaboradores e a criação de programas de proteção de testemunhas digitais são estratégias que contribuem para desarticular redes criminosas sofisticadas e fortalecer a investigação criminal.

No plano educacional, a legislação deve prever medidas de educação digital nas escolas públicas e privadas, com enfoque em segurança online, ética no uso da internet, identificação de fake news, proteção de dados pessoais e prevenção de crimes como aliciamento, bullying virtual, extorsão sexual e fraudes financeiras. A formação cidadã digital é componente essencial de qualquer política criminal moderna, e sua inclusão no currículo escolar representa uma ação preventiva de longo alcance, com impacto direto na redução da criminalidade e na formação de uma cultura de responsabilidade digital entre crianças e adolescentes.

Por fim, as reformas legislativas devem estar acompanhadas de uma estratégia clara de adesão à Convenção de Budapeste, como marco jurídico de inserção do Brasil na cooperação internacional em matéria de cibercrime. A adesão não implica submissão normativa, mas integração a uma rede de compartilhamento de dados, boas práticas e assistência jurídica mútua, que fortalecerá a capacidade de resposta do Estado brasileiro e assegurará sua participação ativa nos fóruns multilaterais de governança digital. A adesão, aliada à atualização legislativa e institucional, permitirá ao Brasil atuar de forma coordenada com os principais países do mundo na repressão a condutas como terrorismo cibernético, espionagem industrial, manipulação eleitoral e lavagem de dinheiro por criptomoedas (Conselho da Europa, 2001).

Em suma, a modernização da legislação cibernética brasileira exige medidas estruturantes e interdependentes. A criação de um código penal digital, a reforma do Código de Processo Penal, a especialização institucional, a formação técnica dos operadores, o fortalecimento do compliance empresarial, a promoção da educação digital e a adesão à Convenção de Budapeste constituem um conjunto coerente e estratégico de reformas que devem ser implementadas com urgência. Somente por meio dessa transformação legislativa profunda e articulada será possível enfrentar, com eficácia e legitimidade, os desafios da criminalidade digital no século XXI.

3.6 A urgência de políticas públicas integradas e programas de prevenção digital

Superar os desafios do cibercrime exige, além de repressão eficaz, uma política de prevenção digital integrada, contínua e coordenada entre Estado, setor privado e sociedade civilA ausência de um plano nacional robusto de prevenção ao cibercrime no Brasil revela um déficit histórico na formulação de políticas públicas voltadas à segurança digital. Embora existam iniciativas isoladas, como as campanhas esporádicas promovidas por órgãos federais e entidades privadas, a inexistência de um arcabouço articulado compromete sua efetividade e alcance. Um modelo eficaz exige a integração de diferentes esferas governamentais – federal, estadual e municipal –, bem como a participação ativa da sociedade civil, do setor privado e do meio acadêmico, todos como corresponsáveis pela construção de uma cultura nacional de cibersegurança.

Portugal, apesar de seus desafios, adota planos nacionais de cibersegurança coordenados pelo CNCS, destacando-se pela integração entre Estado, setor privado e academia, e pela ênfase na prevenção como política pública de longo prazo. No Brasil, a ausência de uma autoridade central com competência plena sobre cibersegurança compromete a coordenação de ações preventivas. Embora existam órgãos com atuações relevantes, como o Gabinete de Segurança Institucional (GSI), a Polícia Federal, a Autoridade Nacional de Proteção de Dados (ANPD) e o Exército Brasileiro (por meio do Comando de Defesa Cibernética), a atuação dispersa e por vezes concorrente entre essas entidades evidencia a necessidade urgente de uma estrutura normativa que institua um plano nacional de prevenção digital, com base legal clara e recursos garantidos por lei orçamentária.

Uma política pública de prevenção ao cibercrime deve, necessariamente, contemplar ações de educação digital desde o ensino básico. A alfabetização digital crítica deve ser incorporada ao currículo escolar como disciplina obrigatória, a fim de formar cidadãos conscientes de seus direitos, deveres e dos riscos do ambiente virtual. Esta proposta encontra eco no modelo da Estônia, que introduziu disciplinas de cidadania digital desde os anos iniciais da escolarização, com resultados concretos na redução de fraudes, crimes de ódio e disseminação de desinformação. A formação digital deve também incluir professores, gestores escolares e famílias, criando uma rede de proteção ativa em torno do uso seguro da tecnologia.

Além disso, a criação de centros de prevenção e resposta rápida a incidentes cibernéticos em nível regional e municipal deve ser tratada como prioridade. Tais centros, inspirados nos *Computer Emergency Response Teams* (*CERTs*) internacionais, funcionariam como núcleos de monitoramento, orientação e suporte técnico às comunidades locais, descentralizando o poder de resposta e promovendo maior capilaridade no enfrentamento às ameaças. Essas unidades poderiam operar em cooperação com universidades e centros tecnológicos, assumindo também papel educativo junto às populações atendidas.

Outro eixo relevante das políticas públicas de prevenção digital deve contemplar a inclusão digital com segurança. O acesso à internet, quando não acompanhado de formação adequada, potencializa vulnerabilidades, sobretudo em populações economicamente desfavorecidas. No Brasil, programas de inclusão digital como o "Computador para Todos" ou "Wi-Fi Brasil", embora positivos, não contemplaram de forma satisfatória os riscos associados à navegação e à exposição de dados. Políticas públicas modernas devem conjugar democratização do acesso com mecanismos protetivos, como sistemas operacionais adaptados, filtros de conteúdo e campanhas de conscientização culturalmente adequadas aos públicos-alvo.

A prevenção também exige atuação incisiva na formação e capacitação continuada dos agentes públicos, especialmente aqueles responsáveis por políticas sociais, educacionais, de saúde e segurança. A intersetorialidade das políticas públicas requer que assistentes sociais, agentes de saúde, conselheiros tutelares, promotores e magistrados estejam preparados para identificar indícios de crimes digitais – como aliciamento, exploração sexual infantil, golpes financeiros e *cyberbullying* – e saibam a quem reportar ou como

intervir de forma ética e eficiente. A formação, nesse contexto, deve ser obrigatória e oferecida pelo Estado, com certificação periódica.

Na esfera legislativa, é necessário prever obrigações legais específicas para a formulação e implementação de planos municipais e estaduais de prevenção digital, estabelecendo parâmetros mínimos de atuação, indicadores de impacto e metas progressivas. A criação de um marco normativo nacional de políticas públicas preventivas, nos moldes da Lei nº 13.257/2016 (Marco Legal da Primeira Infância), permitiria consolidar diretrizes comuns e promover maior equidade entre os entes federativos, hoje extremamente desiguais em capacidade técnica e orçamentária.

Outro aspecto decisivo é a parceria com o setor privado e as grandes plataformas digitais, que devem ser compelidas legalmente a investir em medidas preventivas que extrapolem o âmbito de *compliance*. Não basta que as empresas removam conteúdos ou colaborem com investigações judiciais: é preciso que desenvolvam mecanismos de detecção automática de atividades suspeitas, divulguem relatórios públicos de incidentes e assumam compromissos com campanhas educativas de largo alcance. A responsabilização compartilhada deve estar prevista em lei, com incentivos fiscais para boas práticas e sanções severas para omissões intencionais.

A transversalidade das políticas públicas de prevenção exige também a criação de observatórios de cibercriminalidade e vulnerabilidade digital, compostos por equipes multidisciplinares e integrados a universidades, órgãos de segurança e instituições internacionais. Tais observatórios seriam responsáveis por coletar, sistematizar e analisar dados sobre padrões de ataques, perfis de vítimas, eficácia das campanhas preventivas e impactos sociais dos crimes digitais. A produção de conhecimento empírico qualificado é indispensável para a formulação de políticas baseadas em evidências e para o aprimoramento contínuo das estratégias públicas.

Por fim, a prevenção digital demanda investimento estruturado em campanhas públicas permanentes de conscientização e engajamento, não apenas voltadas para adultos, mas especialmente para jovens, idosos e comunidades vulneráveis. A linguagem deve ser acessível, os canais de divulgação variados e a frequência das campanhas contínua, evitando a sazonalidade que tanto prejudica a fixação das mensagens. O modelo

português, com iniciativas como o "SeguraNet" e o "Media Smart", pode servir de inspiração, desde que adaptado às especificidades brasileiras (SeguraNet, 2024).

A urgência de políticas públicas integradas e programas de prevenção digital não é mais uma escolha política, mas uma imposição da realidade social contemporânea. A falha em responder a esse imperativo coloca o Brasil em posição de vulnerabilidade frente aos desafios da transformação digital. A prevenção não é sinônimo de contenção ou censura, mas de empoderamento social, inclusão segura e proteção integral dos direitos fundamentais no ambiente virtual. Ao deixar de agir preventivamente, o Estado abdica de seu papel constitucional de garantidor da dignidade humana também no ciberespaço.

Capítulo 4 - Discussão dos Resultados

4.1 Estratégias Inovadoras e Reformas Críticas para o Fortalecimento da Legislação Cibernética no Brasil Introdução

A análise empreendida ao longo deste estudo permite afirmar que o ordenamento jurídico brasileiro permanece estruturalmente defasado no que tange à persecução penal dos crimes cibernéticos. Essa defasagem não é meramente técnica, mas revela a ausência de uma política criminal digital robusta, integrada e em consonância com os parâmetros internacionais. Enquanto Portugal consolidou sua legislação e institucionalidade desde 2009 com a Lei n.º 109/2009, o Brasil apenas em 2023 formalizou sua adesão à Convenção de Budapeste por meio do Decreto n.º 11.491, revelando o atraso na harmonização normativa. A adesão brasileira, embora simbólica, ainda não produziu efeitos substantivos na reorganização do sistema penal digital brasileiro.

No contexto legislativo, a Lei nº 12.737/2012, chamada de Lei Carolina Dieckmann, foi concebida para punir invasões a dispositivos eletrônicos, mas sua gênese casuística revela que o enfrentamento ao cibercrime no Brasil foi por muito tempo reativo e desarticulado. Tal legislação é insuficiente para tratar da complexidade dos crimes digitais que envolvem criptografia, redes descentralizadas, dark web e ataques automatizados. Como destacam Almeida e Moura (2022), a legislação brasileira é "um mosaico normativo incapaz de responder à dinamicidade e transnacionalidade do cibercrime" (p. 87). Já Portugal, ao estabelecer um diploma específico e detalhado sobre crimes informáticos, oferece um sistema de prevenção e repressão mais eficaz, respaldado ainda pela

articulação com as estruturas da União Europeia e os mecanismos previstos na Convenção de Budapeste.

A implementação da Convenção de Budapeste em Portugal trouxe reflexos positivos tanto para a tipificação penal quanto para a cadeia probatória. Em solo português, a prova digital é regulamentada por normas específicas, e a atuação das autoridades judiciárias é orientada por protocolos que asseguram a cadeia de custódia digital. No Brasil, por outro lado, ainda não há normatização detalhada sobre como deve ser feita a coleta, preservação e análise da prova eletrônica, o que tem gerado insegurança jurídica e fragilidade processual. Como observam Teixeira e Santos (2023), "a ausência de um protocolo nacional de integridade da prova digital no Brasil compromete sua admissibilidade em juízo, sobretudo nos casos em que a origem dos dados é transnacional" (p. 113).

A diferença de infraestrutura institucional é igualmente notável. Em Portugal, a UNC3T (Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica), vinculada à Polícia Judiciária, é um órgão de referência europeia. Ela atua com equipas forenses especializadas, protocolos de cooperação com a Europol e sistemas de resposta em tempo real. No Brasil, embora existam unidades como o Serviço de Repressão a Crimes Cibernéticos da Polícia Federal, a estrutura ainda é limitada e desigualmente distribuída. Muitas delegacias não têm acesso a especialistas em informática forense, e em diversas comarcas sequer existem técnicos treinados para analisar dispositivos eletrônicos apreendidos.

Dados empíricos sustentam esse descompasso. O relatório da Fortinet (2025) apontou que o Brasil sofreu, em 2024, mais de 100 bilhões de tentativas de ataque cibernético — o maior número da América Latina. No mesmo ano, um levantamento do laboratório da PSafe identificou que cerca de 2,5 milhões de brasileiros foram diretamente prejudicados por vazamentos de dados pessoais, com perdas estimadas em mais de R$ 800 milhões em transações fraudulentas. Além disso, uma pesquisa do DataSenado (2024) revelou que 24% da população adulta do país foi vítima de golpes digitais nos 12 meses anteriores à pesquisa, representando mais de 40 milhões de pessoas lesadas. Esses números evidenciam não apenas a escala do problema, mas a ausência de mecanismos estatais eficazes para prevenção, investigação e punição.

No plano processual, as consequências dessa fragilidade são perceptíveis. Não são raros os casos em que provas digitais obtidas sem os devidos cuidados técnicos são invalidadas judicialmente, mesmo quando demonstram com clareza a autoria e a materialidade delitiva. O Judiciário brasileiro, por vezes, ainda opera sob a lógica das provas tradicionais, não compreendendo plenamente a volatilidade, a replicabilidade e a mutabilidade dos dados eletrônicos. Como destaca Silveira (2021), "a natureza não tangível da prova digital exige do julgador uma mudança paradigmática: da materialidade física para a confiabilidade técnica" (p. 59). Em Portugal, esse paradigma já está consolidado: magistrados, promotores e agentes da Polícia Judiciária passam por formação continuada sobre cibercrime, o que confere maior segurança jurídica e assertividade nas decisões judiciais.

Outro elemento central discutido nesta dissertação é a cooperação internacional. O cibercrime, por definição, é transnacional. A Convenção de Budapeste prevê mecanismos como o ponto de contato 24/7, assistência jurídica mútua e preservação de dados em tempo real. Portugal participa ativamente desses mecanismos, tendo sido elogiado em relatórios do Conselho da Europa pela eficácia de suas respostas a solicitações de outros países. O Brasil, mesmo após a adesão formal, ainda não implementou plenamente os dispositivos de cooperação. Não há até o momento uma estrutura de resposta rápida permanente para pedidos de preservação de dados, o que fragiliza sua capacidade de atuar em crimes envolvendo jurisdições múltiplas.

Além das questões repressivas e processuais, é preciso destacar o papel das políticas públicas preventivas. Em Portugal, políticas de literacia digital estão integradas ao sistema educativo desde o ensino básico. A Estratégia Nacional de Cibersegurança, atualizada em 2023, prevê campanhas periódicas de conscientização, treinamentos interministeriais e parcerias com o setor privado para ampliar a proteção de infraestruturas críticas. No Brasil, ainda que existam iniciativas pontuais, elas não se apresentam de forma articulada. Faltam programas educativos estruturados, investimentos contínuos em capacitação e uma cultura institucional voltada à segurança da informação. Essa lacuna impede a formação de uma cidadania digital consciente e amplifica a vulnerabilidade da população frente às ameaças do ambiente virtual.

4.2 Consolidação de um Código Penal Digital: fundamentos e desafios

Diante da realidade analisada, torna-se inevitável reconhecer que a ausência de um Código Penal Digital representa não apenas uma lacuna jurídica, mas um obstáculo estrutural à construção de uma política criminal eficaz no Brasil. A fragmentação normativa identificada ao longo deste estudo revela que a legislação penal atual não dialoga com a natureza híbrida, descentralizada e transfronteiriça do cibercrime. Ao manter dispositivos dispersos e desarticulados entre si, o ordenamento jurídico brasileiro oferece respostas parciais, por vezes obsoletas, a condutas cuja complexidade exige um tratamento sistemático e tecnicamente calibrado (Bechara, 2020; Florêncio, 2021).

A criação de um Código Penal Digital surge, assim, como um imperativo para a reorganização racional do arcabouço normativo relacionado aos delitos informáticos. Sua função ultrapassaria a simples compilação de tipos penais, assumindo a missão de fundar uma nova racionalidade penal, orientada pelos princípios constitucionais da legalidade, da proporcionalidade e da taxatividade, mas sensível às transformações tecnológicas e à dinamicidade do ciberespaço (Bitencourt, 2022).

O cenário legislativo brasileiro atual está marcado por um conjunto normativo difuso: dispositivos do Código Penal de 1940 convivem com leis específicas como a Lei nº 12.737/2012, o Marco Civil da Internet (Lei nº 12.965/2014) e a LGPD (Lei nº 13.709/2018), sem que exista uma integração lógica e funcional entre essas normas (González, 2019). Como resultado, operadores do direito enfrentam dificuldades interpretativas e práticas, que se traduzem em instabilidade jurisprudencial, insegurança jurídica e baixa efetividade punitiva.

Nesse contexto, a proposta de codificação deve fundamentar-se em três pilares essenciais: (i) a sistematização normativa, reunindo em um único diploma legal os principais tipos penais relacionados ao cibercrime; (ii) a adequação técnico-jurídica, com tipificações claras, atualizadas e dotadas de vocabulário compatível com a linguagem tecnológica, e (iii) a compatibilização com os compromissos internacionais assumidos pelo Estado brasileiro, sobretudo no âmbito da Convenção de Budapeste (Conselho da Europa, 2001; Florêncio, 2021).

A experiência portuguesa, já consolidada por meio da Lei n.º 109/2009, oferece um modelo referencial nesse processo. Sua estruturação em torno de categorias claras – como acesso ilegítimo, interferência em sistemas, sabotagem digital e fraude informática –

permite maior previsibilidade e funcionalidade ao sistema penal, além de conferir segurança jurídica às decisões judiciais (Machado, 2015; González, 2019). O uso de expressões técnicas de escopo aberto, como "entrada", "transmissão" ou "alteração indevida de dados", garante a flexibilidade interpretativa necessária para acompanhar a mutação tecnológica, sem comprometer os limites da legalidade estrita (Bitencourt, 2022).

Ademais, a internacionalização das condutas criminosas impõe um novo paradigma ao direito penal: a extraterritorialidade da norma. É fundamental que o futuro Código Penal Digital brasileiro contenha dispositivos específicos sobre competência penal para crimes que, embora cometidos por meios remotos e sediados no exterior, produzam efeitos jurídicos no território nacional – diretriz já adotada por países como Alemanha e Reino Unido (Dandurand & Munro, 2020).

Outro ponto sensível diz respeito à dosimetria das penas. A variabilidade dos danos provocados por crimes cibernéticos exige respostas penais proporcionais: desde condutas de baixa ofensividade até ataques massivos contra infraestruturas críticas, com potencial de paralisação de serviços essenciais. A ausência de um escalonamento adequado de sanções compromete tanto a justiça do caso concreto quanto a função simbólica da pena (Florêncio, 2021). Um código especializado permitiria, por exemplo, a previsão de agravantes como reincidência digital, uso de redes botnet, manipulação de algoritmos ou ataques a serviços públicos essenciais (Bitencourt, 2022).

O fortalecimento legislativo nesse campo é amplamente recomendado por organismos internacionais. O relatório de avaliação da Convenção de Budapeste de 2021 ressalta que “a adoção de instrumentos legislativos internos consistentes e tecnicamente atualizados é condição sine qua non para uma cooperação internacional eficaz” (UNODC, 2022, p. 45). Países como Espanha, Estônia e Coreia do Sul já trilharam esse caminho, com diplomas legais modernos que garantem interoperabilidade e integração com sistemas globais de combate ao cibercrime (Dandurand & Munro, 2020; Europol, 2022).

No plano institucional, um código estruturado também favorece a formação continuada de profissionais, a estabilidade jurisprudencial e a previsibilidade regulatória, elementos essenciais para a segurança jurídica e para o funcionamento adequado da justiça criminal digital. A França, por exemplo, integrou sua legislação penal digital ao Code Pénal, o que

resultou em maior eficiência decisória e menor grau de litigiosidade recursal (González, 2019).

Do ponto de vista técnico, é recomendável que o novo código adote uma segmentação temática dos crimes, organizando-os, por exemplo, em: (i) crimes contra sistemas e dados (invasão, DDoS, ransomware); (ii) crimes contra a dignidade digital (exposição de dados, pornografia não consensual, discurso de ódio); e (iii) crimes contra a ordem pública e econômica (fraudes online, manipulação de algoritmos financeiros, sabotagem digital) – modelo já adotado no relatório IOCTA da Europol (Europol, 2022).

Diante de todo o exposto, é possível concluir que a consolidação de um Código Penal Digital no Brasil não constitui apenas uma modernização legislativa, mas uma medida estratégica e civilizatória. Trata-se de um passo necessário para adequar o sistema penal à realidade digital, garantir a coerência das respostas jurídicas e reposicionar o país como ator ativo no cenário internacional da cibersegurança e da cooperação jurídica transnacional (Bechara, 2020; Florêncio, 2021).

4.3 Adoção de tecnologias de IA no combate ao cibercrime

A inteligência artificial (IA) emerge como vetor estratégico no enfrentamento ao cibercrime, ao mesmo tempo em que impõe desafios éticos, operacionais e jurídicos de elevada complexidade. Trata-se de uma tecnologia ambivalente: enquanto potencializa a sofisticação das ameaças digitais por meio de ataques automatizados, deepfakes, bots de engenharia social e esquemas de evasão de rastros, também oferece ferramentas poderosas para o Estado na detecção e resposta a condutas ilícitas. No entanto, a adoção de IA para fins de persecução penal requer um arranjo institucional maduro, regulamentação precisa e controle democrático rigoroso (ENISA, 2022).

No Brasil, observa-se um descompasso preocupante entre o avanço tecnológico e a capacidade regulatória e institucional do Estado. Apesar de existirem algumas iniciativas isoladas, como o uso de big data por órgãos fiscais e reconhecimento facial em segurança pública, ainda não há uma política nacional integrada que discipline o uso da IA no combate ao cibercrime. A ausência de diretrizes normativas, de protocolos técnicos e de mecanismos de auditoria independente compromete não apenas a eficácia das ações, mas

a própria legitimidade dos meios de investigação e coleta de prova digital (Almeida, 2022).

Portugal, por sua vez, já iniciou um processo mais sistemático de incorporação da IA às estratégias de cibersegurança, com apoio do Centro Nacional de Cibersegurança (CNCS) e alinhamento às diretrizes da Estratégia Europeia de Inteligência Artificial. Essa integração interinstitucional, que envolve universidades, forças de segurança e centros de inovação, permite o desenvolvimento de modelos preditivos, monitoramento de tráfego anômalo e detecção de padrões maliciosos com maior agilidade, respeitando princípios de proporcionalidade, transparência e governança algorítmica (Comissão Europeia, 2021; CNCS, 2022).

O diferencial da IA no enfrentamento ao cibercrime reside em sua capacidade de operar em tempo real com grandes volumes de dados, extraindo padrões comportamentais e antecipando ameaças antes que elas se consolidem. Ferramentas como machine learning, reconhecimento de padrões, análise preditiva e redes neurais já vêm sendo empregadas com sucesso por centros de excelência internacionais como o European Cybercrime Centre (EC3) e instituições privadas como a IBM e o MIT Lincoln Laboratory (Europol, 2022).

Entre as aplicações mais promissoras estão a detecção precoce de tentativas de intrusão, a identificação de redes automatizadas de ataque (botnets), a análise de metadados em investigações de pornografia infantil, e a atribuição de autoria digital em contextos de anonimato. Além disso, a IA pode contribuir para a eficiência processual ao automatizar a triagem de grandes volumes de dados eletrônicos, reduzindo o tempo de análise de provas e o risco de erro humano (Dandurand & Leppan, 2020).

Entretanto, os riscos inerentes ao uso da IA em processos penais não podem ser negligenciados. A ausência de auditabilidade, a opacidade algorítmica e a possibilidade de decisões baseadas em correlações estatísticas não verificadas colocam em xeque garantias fundamentais como a presunção de inocência, o contraditório e a ampla defesa. Como advertido por Souza (2020), o uso de “caixas-pretas” decisórias no processo penal compromete o devido processo legal e transfere a racionalidade punitiva do juiz para estruturas automatizadas não submetidas ao escrutínio público.

No plano legislativo, o Brasil ainda carece de um marco normativo específico para regular a aplicação de IA na segurança pública e no processo penal. O Projeto de Lei nº 21/2020, conhecido como Marco Legal da Inteligência Artificial, ainda em tramitação, carece de dispositivos claros sobre responsabilidade, auditabilidade e transparência nos usos estatais dessas tecnologias (Pereira & Costa, 2023). A ausência dessa normatização fragiliza a legalidade dos atos investigativos e pode levar à invalidação de provas colhidas por meios automatizados.

A União Europeia, por sua vez, avançou no desenvolvimento do AI Act – uma regulamentação robusta que estabelece níveis de risco e exigências proporcionais conforme a natureza da aplicação. Sistemas de IA considerados de "alto risco", como os usados em processos penais e segurança pública, devem ser registrados, auditados, explicáveis e sujeitos à responsabilização institucional (Comissão Europeia, 2022). Esse modelo normativo oferece uma referência valiosa para o Brasil, que pode adaptá-lo às suas particularidades federativas.

É urgente, portanto, a construção de uma política pública nacional voltada à pesquisa, desenvolvimento e uso ético da IA na cibersegurança. Tal política deve se assentar sobre três pilares fundamentais: (i) fomento à pesquisa aplicada por universidades públicas em parceria com órgãos de segurança; (ii) criação de centros interinstitucionais de ciberinteligência para desenvolvimento e validação de soluções tecnológicas; e (iii) regulamentação técnica e jurídica da IA aplicada à persecução penal, com auditoria obrigatória e responsabilização objetiva do Estado por eventuais abusos (Souza, 2020).

Por fim, é necessário destacar o papel do setor privado, que detém não apenas a maior parte das tecnologias, mas também a responsabilidade sobre plataformas onde ocorrem diversos delitos digitais. A resistência das grandes corporações em adotar IA para fins de prevenção criminal – enquanto amplamente a utilizam para segmentação de mercado e publicidade – expõe um desequilíbrio ético que precisa ser enfrentado pelo legislador. O modelo alemão da NetzDG e os debates atuais em Portugal sobre a responsabilização de intermediários digitais apontam caminhos possíveis para essa regulação (Silva, 2022).

A IA não pode ser vista como substituta da atuação humana, mas como ferramenta complementar que exige vigilância democrática e técnica constante. Sua incorporação ao

sistema de justiça penal digital deve ser conduzida com prudência, transparência e compromisso inegociável com os direitos fundamentais.

4.4 Os desafios da responsabilização penal nos crimes cibernéticos: entraves técnicos e lacunas processuais

A responsabilização penal nos crimes cibernéticos é um dos pontos mais críticos e reveladores da fragilidade estrutural do sistema de justiça criminal brasileiro frente à nova lógica delitiva digital. Ainda que se observe uma crescente tipificação de condutas no plano normativo, a prática revela entraves técnicos que comprometem, de modo recorrente, a efetividade da persecução penal. Trata-se de uma realidade marcada por nulidades processuais, arquivamentos por vícios técnicos e absolvições motivadas por deficiências na produção de prova digital (Pereira & Almeida, 2022).

A análise empreendida ao longo deste estudo evidenciou que o arcabouço processual vigente – fortemente baseado em premissas do direito penal tradicional – não oferece respostas adequadas às exigências específicas da cadeia de custódia digital. A inexistência de uma regulamentação técnica que defina, por exemplo, os procedimentos de espelhamento forense, armazenamento seguro de dados e validação pericial compromete a integridade da prova e amplia a margem para sua invalidação judicial. Em diversos casos, mesmo com indícios robustos de autoria, a materialidade digital é desconsiderada por ausência de confiabilidade técnica no processo de coleta e preservação (Souza, 2020).

Além disso, a carência de peritos especializados e a precariedade estrutural dos institutos de criminalística, sobretudo fora dos grandes centros, tornam a investigação criminal digital um processo lento, desarticulado e frequentemente inconclusivo. As falhas não se restringem à esfera policial, estendendo-se ao Ministério Público, onde ainda são raros os núcleos técnicos preparados para lidar com investigações cibernéticas complexas. Muitos promotores, sem formação específica, atuam sob a lógica de delitos convencionais, desconsiderando elementos essenciais como anonimização de IPs, criptografia, uso de VPNs e mecanismos de ofuscação de dados (Florêncio, 2021).

A jurisprudência brasileira, por sua vez, ainda carece de uniformidade e maturidade no trato das provas digitais. É comum encontrar decisões divergentes sobre temas centrais, como validade de registros extraídos de aplicativos de mensagens, admissibilidade de

prints de tela, interceptações em nuvem e coleta de dados sem ordem judicial. Essa instabilidade interpretativa compromete a previsibilidade das decisões e desestimula a atuação firme dos órgãos de persecução penal (Pereira & Almeida, 2022).

Portugal, embora enfrente desafios semelhantes, demonstra maior coesão institucional no enfrentamento dessas lacunas. Desde a promulgação da Lei n.º 109/2009, que internalizou a Convenção de Budapeste, o país desenvolveu protocolos padronizados de preservação da prova digital, com articulação entre Polícia Judiciária, Ministério Público e centros forenses especializados (Machado, 2015). A certificação técnica desses centros, aliada à fiscalização regular e à capacitação contínua dos operadores, resulta em maior legitimidade probatória e menor índice de invalidação judicial.

No Brasil, a ausência de uma norma processual própria sobre a cadeia de custódia digital constitui um vácuo normativo com efeitos processuais diretos. A análise revelou que, mesmo em casos gravíssimos – como pornografia infantil ou ataques a sistemas públicos – provas são desconsideradas judicialmente por falhas formais na perícia ou ausência de protocolo padronizado. A fragilidade institucional é acentuada pela inexistência de linhas de financiamento estáveis para a modernização dos equipamentos forenses, o que torna os laudos imprecisos ou tecnicamente frágeis (Souza, 2020).

A formação de magistrados representa outra barreira significativa. Cursos de formação inicial e continuada raramente incluem disciplinas voltadas ao tratamento jurídico da prova digital, o que leva muitos juízes a interpretarem elementos tecnológicos sob uma ótica analógica. A consequência prática é a proliferação de decisões baseadas no livre convencimento desvinculado de critérios técnicos objetivos, o que reduz a segurança jurídica e prejudica a consolidação de precedentes consistentes (Florêncio, 2021).

A responsabilidade penal em crimes digitais também esbarra na dificuldade de atribuição de autoria, sobretudo nos casos que envolvem o uso de técnicas sofisticadas de ocultação de identidade. A ausência de cooperação internacional ágil – decorrente da não implementação de instrumentos da Convenção de Budapeste, como o ponto de contato 24/7 – limita o acesso a registros essenciais localizados em servidores estrangeiros, enfraquecendo a linha acusatória mesmo quando há elementos indiciários consistentes (Dandurand & Munro, 2020).

No plano internacional, diversos países vêm avançando na construção de marcos processuais específicos para a validade da prova digital, incluindo critérios como rastreabilidade, integridade dos dados, redundância forense e armazenamento seguro. Modelos como os adotados por Alemanha, Canadá e França mostram que a padronização técnica e a formação especializada são requisitos fundamentais para a responsabilização penal efetiva em ambiente digital (Souza, 2020).

Particularmente alarmante é o cenário dos crimes de pornografia infantil digital. A análise demonstrou que, em muitos casos, a ausência de protocolos técnicos rigorosos resulta na invalidação de provas extremamente sensíveis, gerando impunidade em condutas de elevada gravidade. A coleta inadequada, o espelhamento incompleto ou a manipulação não intencional de arquivos digitais por equipes despreparadas têm conduzido à anulação de prisões e ao arquivamento de inquéritos com forte conteúdo probatório (Dandurand & Munro, 2020).

A superação desse cenário exige a elaboração urgente de uma norma processual penal digital no Brasil. Essa normativa deve estabelecer requisitos técnicos mínimos para validade da prova eletrônica, protocolos padronizados de cadeia de custódia e critérios de admissibilidade baseados em parâmetros internacionais. Além disso, é fundamental que Ministério Público e Judiciário incorporem planos de formação obrigatória em cibercriminalidade como condição para atuação em casos que envolvam evidências digitais (Pereira & Almeida, 2022).

A responsabilização penal em crimes cibernéticos não pode ser reduzida a um problema técnico. Ela é expressão direta da capacidade do Estado de exercer sua função protetiva em um ambiente cada vez mais virtualizado. A atual incapacidade de lidar com as especificidades do ciberespaço não apenas enfraquece o sistema de justiça, como transmite à sociedade a mensagem de que determinados delitos permanecem fora do alcance da lei. Corrigir esse cenário é condição elementar para restabelecer a confiança institucional e a credibilidade do Direito Penal.

4.5 A especialização do Judiciário e do Ministério Público como resposta à impunidade digital

A constatação recorrente de impunidade nos crimes cibernéticos, mesmo diante de normas penais já existentes, revela que o problema não se limita à insuficiência legislativa, mas decorre, sobretudo, da inabilidade institucional em lidar com as complexidades técnicas do fenômeno digital. No cerne desse déficit está a ausência de especialização dos principais atores da persecução penal: o Judiciário e o Ministério Público. Ambos, salvo raras exceções, seguem operando a partir de um repertório analógico que se mostra absolutamente ineficaz diante das exigências tecnológicas impostas pela nova criminalidade (Souza, 2020).

A análise realizada confirma que, sem uma estrutura especializada, a responsabilização penal em delitos cibernéticos torna-se frágil, morosa e, frequentemente, inócua. O desconhecimento técnico de juízes e promotores em temas como criptografia, engenharia reversa, rastreamento de IPs, cadeias de custódia digital e armazenamento em nuvem impede a compreensão adequada das provas, o correto enquadramento jurídico das condutas e a aplicação proporcional das garantias constitucionais (Florêncio, 2021). A consequência é a produção de decisões inseguras, nulidades processuais e arquivamentos decorrentes de falhas evitáveis.

Portugal oferece um modelo funcional de enfrentamento desse desafio. A criação de departamentos especializados no Ministério Público, com formação jurídica e tecnológica integrada, permitiu maior eficácia na análise técnica das denúncias, na articulação com a Polícia Judiciária e na preservação da cadeia probatória. Desde a transposição da Convenção de Budapeste em 2009, procuradores com expertise em cibercrime atuam com autonomia técnica e acesso direto a consultores forenses, o que confere agilidade, segurança jurídica e acerto nas decisões acusatórias (Silva, 2022).

A literatura especializada corrobora que a especialização institucional é elemento central para qualificar a atuação do sistema de justiça penal. Experiências como a da Alemanha, França e Países Baixos – onde há seções específicas para cibercrime nos tribunais superiores – demonstram que a presença de magistrados com formação tecnológica reduz significativamente o número de decisões anuladas, fortalece a jurisprudência técnica e facilita o diálogo internacional em casos de jurisdição múltipla (ENISA, 2022; Dandurand & Munro, 2020).

No Brasil, ainda que existam algumas promotorias e delegacias especializadas em crimes digitais em capitais como São Paulo e Curitiba, esses esforços permanecem fragmentados, carentes de padronização normativa e sujeitos à instabilidade funcional. Não há, até o momento, regulamentação nacional que discipline a criação de varas judiciais voltadas exclusivamente à cibercriminalidade, tampouco programas institucionais de formação técnica continuada. A ausência de critérios objetivos de nomeação, de acesso a peritos vinculados às unidades e de redes de compartilhamento técnico impede a consolidação de um corpo jurisprudencial estável e qualificado (Pereira & Almeida, 2022).

A proposta de especialização requer, necessariamente, a definição de três eixos estruturantes: (i) delimitação clara da competência temática das unidades especializadas, com abrangência sobre delitos cibernéticos e questões relativas à prova digital; (ii) criação de programas obrigatórios de capacitação para magistrados e membros do Ministério Público, por meio das Escolas da Magistratura e das Escolas Superiores do MP, com conteúdos validados por especialistas externos; e (iii) estruturação de equipes técnicas permanentes de apoio, com peritos forenses vinculados diretamente às unidades judiciais e ministeriais, conforme modelo aplicado com êxito pela Procuradoria-Geral da República de Portugal (Silva, 2022).

A análise dos dados aponta que a ausência de especialização tem impacto direto na insegurança jurídica. Erros técnicos cometidos por desconhecimento geram decisões contraditórias, nulidades por vícios formais, perda de elementos probatórios e retrabalho judicial, além de comprometerem a credibilidade do sistema. Estudo do UNODC (2021) evidencia que tribunais especializados apresentam menor índice de reversão de decisões em segunda instância e maior aderência a parâmetros técnicos, o que reforça a legitimidade institucional e racionaliza o trâmite processual.

Além da melhoria da performance institucional, a especialização influencia positivamente a formulação de políticas públicas. A jurisprudência produzida por unidades técnicas especializadas contribui para relatórios legislativos, para a elaboração de anteprojetos e para a definição de prioridades normativas no campo penal digital. Países como Canadá e Austrália, assim como os Estados-membros da União Europeia, utilizam tais decisões como base para atualização normativa e aperfeiçoamento de estratégias nacionais de segurança digital (Dandurand & Munro, 2020).

Do ponto de vista prático, a ausência de operadores especializados compromete a proteção das vítimas, favorece a reincidência e aprofunda o sentimento de impunidade. Quando prisões são revogadas por vícios técnicos, quando provas são invalidadas por falhas na cadeia de custódia ou quando denúncias são rejeitadas por deficiências na imputação, o sistema penal revela sua ineficácia frente ao novo paradigma da criminalidade digital (Souza, 2020). A especialização, nesses casos, não é um luxo institucional, mas uma exigência democrática.

É imperativo, portanto, que sejam definidos critérios objetivos para a criação e manutenção dessas estruturas, com indicadores de desempenho, programas de capacitação contínua e participação ativa em redes de cooperação internacionais, como a European Judicial Cybercrime Network e a Global Forum on Cyber Expertise. O enfrentamento da criminalidade digital exige operadores do direito capazes de compreender a lógica técnica das infrações, dominar os instrumentos legais disponíveis e articular respostas eficazes e legítimas em um ambiente transnacional.

A especialização do Judiciário e do Ministério Público é, enfim, um dos pilares fundamentais da soberania digital. Em um cenário global marcado por algoritmos maliciosos, redes de anonimização, inteligência artificial criminosa e mercados ilícitos online, a formação técnica dos operadores jurídicos é condição elementar para a preservação das garantias constitucionais e para a efetividade da justiça penal contemporânea.

4.6 A proteção de infraestruturas críticas e o papel do setor privado

A análise empreendida no decorrer deste estudo permitiu constatar que a proteção das infraestruturas críticas, embora reconhecida em discursos institucionais como elemento estratégico da soberania nacional, ainda se apresenta no Brasil como um campo normativo e operacional vulnerável. Essa fragilidade afeta diretamente a capacidade do Estado de reagir a ciberataques de alta complexidade, compromete serviços essenciais e amplia os riscos sistêmicos decorrentes da crescente digitalização de setores como energia, finanças, comunicações e transportes (ENISA, 2022).

Os dados revelam que a inexistência de um marco legal específico e vinculativo para a proteção de infraestruturas críticas no Brasil gera lacunas normativas que dificultam a

coordenação interinstitucional e reduzem a eficácia das respostas em caso de incidentes de grande escala. O Decreto nº 10.569/2020, embora tenha instituído a Estratégia Nacional de Segurança Cibernética (E-Ciber), limita-se a traçar diretrizes genéricas, sem impor obrigações técnicas, protocolos mandatórios ou mecanismos de responsabilização aos agentes envolvidos (TCU, 2021).

O contraste com o modelo europeu – em especial com a Diretiva NIS e sua transposição em Portugal pela Lei n.º 46/2018 – é marcante. A legislação portuguesa define com clareza quem são os operadores de serviços essenciais, quais são suas responsabilidades, quais padrões mínimos devem adotar em termos de segurança da informação e quais as consequências do não cumprimento dessas obrigações. Além disso, institui auditorias externas regulares e prevê mecanismos de notificação imediata de incidentes, criando um sistema robusto de prevenção e resposta a riscos cibernéticos (Comissão Europeia, 2021).

A ausência de uma autoridade reguladora centralizada e tecnicamente competente no Brasil compromete a padronização de protocolos e a interoperabilidade entre os setores. Atualmente, as responsabilidades estão dispersas entre agências reguladoras setoriais como ANEEL, ANATEL, ANP e Banco Central, que operam de maneira isolada e com exigências muitas vezes desconectadas das realidades técnicas e jurídicas do ciberespaço (Pereira & Almeida, 2022). Esse descompasso institucional compromete a formação de uma cultura nacional de cibersegurança e dificulta o compartilhamento de informações estratégicas em tempo real.

A investigação revelou, ainda, que parte significativa da infraestrutura crítica brasileira está sob gestão do setor privado, o que torna sua corresponsabilização indispensável. No entanto, as empresas frequentemente resistem à cooperação com o poder público, alegando sigilo comercial, ausência de obrigação legal ou incompatibilidade técnica com os sistemas oficiais. Tal postura, além de comprometer investigações e ações de contenção de danos, revela a carência de um regime jurídico que defina com precisão os deveres dos agentes privados diante de ameaças cibernéticas (Souza, 2023).

Nesse sentido, Portugal oferece um modelo de governança compartilhada exemplar, por meio do Centro Nacional de Cibersegurança (CNCS), que atua como elo de integração entre o setor público, a iniciativa privada e os centros de pesquisa. A atuação do CNCS inclui o fomento à cultura de segurança digital, a capacitação técnica dos gestores de

infraestrutura, a realização de simulações regulares de incidentes e a emissão de alertas coordenados. Essa estrutura permite respostas mais rápidas, integradas e legitimadas socialmente (CNCS, 2022).

No Brasil, por outro lado, investigações relatadas pelo Ministério Público Federal revelam que empresas de telecomunicações e plataformas digitais não apenas demoram a cumprir ordens judiciais como, em muitos casos, alegam a impossibilidade técnica de fornecer dados essenciais para a persecução penal, por ausência de logs ou pela alegada expiração de prazos internos de retenção. Essa fragilidade probatória, aliada à inexistência de normas específicas sobre preservação de dados em contextos de infraestruturas críticas, amplia os riscos de impunidade e enfraquece a autoridade estatal (Pereira & Almeida, 2022).

Embora a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) represente um avanço no que tange à proteção de informações pessoais, ela não trata, de modo específico, da segurança de sistemas estruturantes do Estado. Essa lacuna normativa deixa desprotegidas as bases operacionais que sustentam o funcionamento da sociedade contemporânea, como sistemas de abastecimento de água, controle aéreo, rede elétrica, bancos de dados públicos e plataformas de autenticação digital (Souza, 2023).

A construção de um marco legal voltado à proteção de infraestruturas críticas deve contemplar: (i) definição clara e atualizada do que constitui infraestrutura crítica; (ii) imposição de requisitos técnicos mínimos de segurança digital; (iii) criação de protocolos obrigatórios de resposta e notificação; (iv) mecanismos de fiscalização com poder sancionador e (v) incentivos regulatórios para a adoção voluntária de padrões superiores de resiliência. Tal marco permitiria consolidar uma política pública articulada e integrada de defesa digital estratégica.

Outro elemento essencial identificado foi a necessidade de um sistema nacional de avaliação da maturidade cibernética, inspirado em modelos como o CMMC (Cybersecurity Maturity Model Certification) dos EUA ou o MARC (Modelo de Avaliação da Resiliência Cibernética) de Portugal. Esses sistemas não apenas promovem benchmarking e transparência entre os operadores, mas estimulam melhorias contínuas na governança digital, mediante índices comparativos e certificações de conformidade (CNCS, 2022).

A institucionalização de CSIRTs (Computer Security Incident Response Teams) setoriais, com gestão híbrida público-privada, também se mostra uma estratégia indispensável para garantir vigilância contínua, resposta imediata a ataques e recuperação coordenada de sistemas críticos. Países como Estônia, Finlândia e França já operam com estruturas dessa natureza, promovendo uma cultura de resiliência compartilhada e preventiva (ENISA, 2022).

O papel do setor privado, portanto, não pode mais ser compreendido como meramente reativo ou auxiliar. As empresas que operam em segmentos estratégicos da economia devem assumir obrigações regulatórias, participar de estruturas conjuntas de defesa cibernética e responder, de forma objetiva, por omissões que comprometam a segurança nacional digital. Essa corresponsabilidade precisa estar prevista em lei, ancorada em protocolos técnicos e legitimada por práticas auditáveis.

A vulnerabilidade das infraestruturas críticas brasileiras, aliada à ausência de normas claras e à resistência do setor privado à cooperação estruturada, revela que o país ainda não incorporou a cibersegurança como um componente essencial da segurança do Estado. Sem uma legislação moderna, mecanismos de responsabilização e estruturas de coordenação técnica, o Brasil continuará exposto a riscos sistêmicos, cujas consequências podem afetar não apenas sua estabilidade institucional, mas a própria integridade de sua soberania digital.

Assim, ao integrar os achados empíricos, as fragilidades normativas e os contrastes institucionais entre Brasil e Portugal, torna-se evidente que os desafios enfrentados pela legislação cibernética nacional ultrapassam as fronteiras do campo jurídico, exigindo uma profunda reestruturação do aparato institucional e um redimensionamento das estratégias políticas de enfrentamento à criminalidade digital. As propostas delineadas ao longo desta discussão não pretendem esgotar o tema, mas evidenciam, com base em fundamentos teóricos e exemplos práticos, que a persistência de um modelo fragmentado, analógico e descoordenado tende apenas a ampliar o déficit de proteção jurídica e a comprometer a legitimidade do sistema penal frente às novas demandas da era digital. No capítulo seguinte, serão sistematizadas as conclusões finais deste trabalho, com ênfase nas reformas legislativas, nos deveres de cooperação internacional e na necessidade de modernização tecnológica e institucional como condição de sobrevivência do próprio Estado de Direito em tempos de cibercriminalidade transnacional.

Capítulo 5 - Estudo Empírico Documental: Análise Comparativa das Estruturas Legislativas de Brasil e Portugal no Combate ao Cibercrime

A presente seção empírica da dissertação tem por finalidade aprofundar a análise comparativa entre os ordenamentos jurídicos brasileiro e português no enfrentamento à criminalidade cibernética, por meio de um estudo documental rigorosamente conduzido. Esta etapa da pesquisa se ancora metodologicamente na análise de normas legais e tratados internacionais vigentes, cuja interpretação permitirá compreender como cada país estrutura sua política criminal diante de um cenário de ameaças digitais complexas e em contínua evolução. A pesquisa parte da premissa de que o direito positivo — especialmente as leis penais, processuais e os compromissos internacionais ratificados — constitui objeto legítimo de observação empírica, desde que analisado com critérios científicos claros, objetivos e comparáveis.

A seguir, são apresentados os fundamentos do estudo empírico, seus objetivos específicos, a metodologia adotada e, posteriormente, os resultados observados e sua discussão crítica, de forma a garantir a conformidade metodológica exigida e a máxima transparência na construção analítica da investigação.

5.1 Fundamentação

A construção de um estudo empírico sobre cibercriminalidade demanda uma base teórica sólida que legitime a análise documental como método científico válido. No campo da Criminologia, a utilização de fontes normativas e institucionais como corpus empírico tem sido amplamente reconhecida, sobretudo em investigações voltadas à compreensão da resposta penal diante de fenómenos complexos e em constante mutação, como o crime cibernético. A análise documental permite identificar, com objetividade, as estruturas legais e processuais em vigor, bem como os compromissos internacionais assumidos pelos Estados, revelando não apenas os aspetos formais das normas, mas também as suas omissões, contradições e fragilidades práticas.

No caso específico desta pesquisa, fundamenta-se a análise documental nas exigências metodológicas da Universidade Fernando Pessoa, que admite expressamente estudos empíricos baseados em fontes normativas, desde que haja clareza metodológica, rigor de seleção e interpretação crítica das fontes. O objeto da análise — a legislação penal de

Brasil e Portugal relativa ao enfrentamento do cibercrime — é considerado empiricamente verificável, pois está materializado em códigos, leis, decretos e tratados oficialmente promulgados. Tais documentos refletem, de forma concreta, a política criminal adoptada em cada país frente às novas ameaças do ambiente digital.

A pertinência da comparação entre Brasil e Portugal justifica-se pela afinidade linguística e histórica entre os dois ordenamentos jurídicos, bem como pela diferença significativa no grau de adesão e internalização da Convenção sobre o Crime Cibernético (Convenção de Budapeste). Portugal ratificou e implementou a Convenção desde 2010, enquanto o Brasil somente a promulgou em 2023 por meio do Decreto n.º 11.491, de 12 de abril de 2023. Este decreto, publicado no Diário Oficial da União, promulga oficialmente a Convenção sobre o Crime Cibernético firmada em Budapeste, tornando-a parte integrante do ordenamento jurídico brasileiro.

A sua promulgação representa não apenas um marco simbólico, mas também jurídico, pois transforma compromissos internacionais em obrigações normativas internas e impõe ao Brasil o dever legal de harmonizar a sua legislação penal e processual aos padrões estabelecidos pelo Conselho da Europa. O Decreto n.º 11.491/2023 estabelece os fundamentos formais para a internalização de medidas como a tipificação penal mínima comum, a preservação célere de dados eletrónicos, a cooperação internacional imediata e o uso de instrumentos de assistência mútua para obtenção de provas digitais transnacionais. Trata-se, portanto, de um dispositivo normativo com repercussões práticas diretas sobre a actuação de autoridades judiciais, policiais e do Ministério Público, exigindo atualização técnica e institucional por parte dos operadores do Direito.

A defasagem de mais de uma década entre a ratificação portuguesa e a promulgação brasileira evidencia uma assimetria que permite, sob o ponto de vista académico, analisar os efeitos práticos de uma adesão precoce versus uma adesão tardia à mesma convenção internacional. Enquanto Portugal já consolidou canais operacionais como a Rede 24/7, o Eurojust e o e-Evidence, o Brasil inicia agora o processo de estruturação e articulação para aceder a tais mecanismos com respaldo normativo consolidado. Assim, o Decreto n.º 11.491/2023 não pode ser compreendido como mero acto administrativo: ele simboliza o início de uma reconfiguração estratégica da política criminal brasileira frente às ameaças do ciberespaço, e a sua análise empírica é indispensável para avaliar as

condições reais da sua aplicação, os seus desafios interpretativos e os seus impactos sobre o sistema penal.

Ademais, a fundamentação empírica desta análise encontra suporte em estudos normativos que reconhecem o Direito como objecto legítimo de observação empírica, tal como defendido por Norberto Bobbio, Hans Kelsen e Günther Jakobs, na medida em que o direito positivo é um dado social estruturante. Ao abordar as normas como instrumentos operacionais do sistema penal, a presente pesquisa enquadra-se dentro da tradição criminológica crítica, que busca compreender os limites e os alcances da punição estatal diante de novas modalidades de delinquência. A legislação penal, portanto, não é aqui apenas um conjunto abstracto de textos, mas um reflexo das escolhas político-criminais de cada país diante de ameaças tecnológicas globais.

5.2 Objetivos

O presente estudo empírico tem como objetivo central comparar as estruturas legislativas do Brasil e de Portugal no enfrentamento ao cibercrime, com base em documentos normativos oficialmente promulgados por ambos os países. A análise visa identificar as convergências e divergências entre os dois ordenamentos, com foco especial na incorporação e na efetividade das diretrizes previstas na Convenção sobre o Crime Cibernético, adotada em Budapeste no ano de 2001 e ratificada por Portugal em 2010 e pelo Brasil apenas em 2023, por meio do Decreto nº 11.491.

O presente estudo empírico tem como objetivo central comparar as estruturas legislativas do Brasil e de Portugal no enfrentamento ao cibercrime, com base em documentos normativos oficialmente promulgados por ambos os países. A análise visa identificar as convergências e divergências entre os dois ordenamentos, com foco especial na incorporação e na efetividade das diretrizes previstas na Convenção sobre o Crime Cibernético, adotada em Budapeste no ano de 2001. De forma específica, pretende-se avaliar a completude, coerência e atualização da legislação penal brasileira e portuguesa relativa ao cibercrime, considerando os principais diplomas legais de cada país; verificar o grau de aderência de cada sistema normativo às exigências estabelecidas pela Convenção de Budapeste, com destaque para os aspectos penais e processuais; analisar as lacunas normativas presentes no Brasil e em Portugal, especialmente no que se refere à tipificação de condutas, à produção de prova digital e à cooperação internacional;

compreender os impactos concretos da ratificação tardia da Convenção pelo Brasil, e como essa demora legislativa afeta a eficácia do combate à criminalidade cibernética; e contribuir com subsídios técnico-científicos para futuras propostas legislativas e políticas públicas, com base na experiência portuguesa e nas exigências internacionais já assumidas pelo Estado brasileiro.

Ao estabelecer tais objetivos, o estudo não apenas cumpre o requisito metodológico de um trabalho empírico na área da Criminologia, mas também pretende oferecer um diagnóstico crítico e propositivo, fundamentado em dados normativos concretos e na realidade institucional observável nos dois contextos jurídicos analisados.

5.3 Metodologia

A presente investigação empírica caracteriza-se por uma abordagem qualitativa de natureza documental e comparativa, centrada na análise de normas jurídicas e instrumentos legais oficialmente promulgados em Portugal e no Brasil no âmbito do combate à criminalidade cibernética. A escolha dessa metodologia está diretamente associada ao objeto do estudo, que se fundamenta em fontes primárias do direito positivo e internacional, legitimando a utilização da análise documental como ferramenta científica adequada para examinar a resposta institucional dos ordenamentos jurídicos à cibercriminalidade contemporânea.

Foram selecionados como documentos de análise as legislações penais vigentes, as normas processuais relevantes, os tratados internacionais ratificados, decretos de promulgação e, particularmente, a Convenção sobre o Crime Cibernético, firmada em Budapeste, adotada por Portugal em 2010 e promulgada pelo Brasil somente em 2023 por meio do Decreto nº 11.491. Entre os instrumentos legais analisados, destacam-se o Código Penal português, a Lei nº 109/2009 (Lei do Cibercrime), o Código Penal brasileiro, a Lei nº 12.737/2012 (Lei Carolina Dieckmann), o Marco Civil da Internet (Lei nº 12.965/2014), a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), bem como o Regulamento Geral sobre a Proteção de Dados da União Europeia. Estes textos normativos foram extraídos diretamente de fontes oficiais, como os sites das assembleias legislativas, diários oficiais e plataformas jurídicas estatais, garantindo sua veracidade e integridade.

A análise comparativa foi realizada por meio da identificação e categorização temática de aspectos jurídicos comuns, divergentes e ausentes nos dois ordenamentos. Os documentos foram examinados quanto à existência e ao detalhamento de tipificações penais específicas para crimes digitais, às previsões sobre prova digital, às normas processuais relativas à investigação e à obtenção de dados eletrônicos, e às medidas de cooperação internacional previstas em cada país. Embora a pesquisa não envolva seres humanos como participantes diretos, os sujeitos institucionalmente observados são os próprios sistemas jurídicos de Brasil e Portugal, compreendidos como estruturas normativas organizadas que expressam escolhas político-criminais distintas frente ao mesmo desafio global.

O procedimento adotado consistiu na leitura sistemática dos dispositivos legais à luz dos compromissos internacionais assumidos por cada país, especialmente no que diz respeito à harmonização legislativa com a Convenção de Budapeste. A coleta e seleção dos documentos ocorreu entre janeiro e abril de 2025, sendo priorizados textos atualizados e reconhecidos oficialmente. A análise foi conduzida com base em critérios de aderência normativa, coerência interna, completude legislativa e operacionalidade jurídico-processual, com atenção especial às implicações práticas da promulgação do Decreto nº 11.491 no Brasil.

A opção pela metodologia documental comparativa justifica-se pelo fato de que as normas jurídicas, quando analisadas de forma sistematizada, oferecem um campo empírico legítimo para a observação do fenômeno jurídico-criminal. Essa abordagem permite extrair inferências sobre a efetividade legislativa e identificar zonas de conflito, omissão ou insuficiência normativa, em linha com o escopo crítico da Criminologia contemporânea. Ao integrar a leitura formal dos textos legais com a compreensão da realidade institucional a que se referem, a presente metodologia revela-se compatível com o objetivo central da pesquisa: interpretar, com rigor técnico e fundamento teórico, as diferentes formas pelas quais Brasil e Portugal enfrentam, no plano normativo, a complexidade crescente do cibercrime.

5.4 Resultados

A análise documental comparativa revelou disparidades significativas entre as estruturas normativas de Brasil e Portugal no que se refere ao enfrentamento jurídico da

criminalidade cibernética. Enquanto Portugal apresenta um corpo legislativo consolidado, estruturado e harmonicamente integrado à Convenção sobre o Crime Cibernético de Budapeste, o Brasil ainda opera com um modelo legislativo fragmentado, tardio e carente de sistematização técnico-jurídica.

No ordenamento jurídico português, observou-se a existência de um diploma específico, a Lei n.º 109/2009, que trata de forma direta e abrangente das infrações penais praticadas por meio de sistemas informáticos. Essa legislação, promulgada com base na Convenção de Budapeste, fornece definições precisas para condutas como acesso ilegítimo, interferência em dados, sabotagem informática e interceção ilegal, além de estabelecer procedimentos processuais próprios para obtenção e conservação de provas digitais. A Lei do Cibercrime integra-se com eficácia ao Código Penal e ao Código de Processo Penal português, formando um sistema coeso que permite respostas rápidas, legítimas e proporcionais por parte das autoridades competentes.

Já no Brasil, a análise documental evidenciou a ausência de um diploma jurídico específico sobre cibercrime. A legislação penal brasileira ainda depende de dispositivos dispersos, como o artigo 154-A do Código Penal (introduzido pela Lei nº 12.737/2012), a Lei Geral de Proteção de Dados (LGPD), o Marco Civil da Internet e outras normas complementares. Embora esses instrumentos contenham previsões relevantes, eles não constituem um sistema normativo integrado, nem foram estruturados sob uma lógica unificada de política criminal. Tal fragmentação dificulta a atuação coordenada das instituições policiais, do Ministério Público e do Poder Judiciário, comprometendo a efetividade da persecução penal no contexto digital.

Outro resultado relevante da análise documental refere-se ao processo de adesão e incorporação da Convenção de Budapeste pelos dois países. Portugal ratificou a convenção em 2009 e, desde então, mantém mecanismos permanentes de atualização normativa, cooperação internacional e adequação técnica da legislação interna. O país é membro ativo de redes europeias de enfrentamento à cibercriminalidade, como o Eurojust e o European Cybercrime Centre (EC3), com atuação reconhecida em operações conjuntas. O Brasil, por outro lado, somente passou a integrar formalmente a convenção em 2023, por meio do Decreto nº 11.491. Até então, o país atuava à margem dos mecanismos internacionais padronizados de cooperação e resposta penal conjunta. Essa

entrada tardia limitou, por anos, a participação do Brasil em canais prioritários de intercâmbio técnico e judicial.

A análise também demonstrou que, do ponto de vista da responsabilização penal de pessoas jurídicas, Portugal adota um modelo mais avançado, prevendo expressamente a possibilidade de responsabilização criminal de empresas envolvidas em infrações informáticas, conforme disposto no artigo 11.º da Convenção de Budapeste e reproduzido na legislação nacional. No Brasil, embora haja previsão de responsabilidade administrativa e civil de pessoas jurídicas em outros contextos (como na Lei Anticorrupção), ainda não há consenso doutrinário nem jurisprudência consolidada quanto à responsabilização penal de empresas por delitos cibernéticos. Essa omissão normativa representa um obstáculo adicional à repressão efetiva de crimes praticados por intermédio de estruturas empresariais ou plataformas tecnológicas.

No que tange à proteção de dados pessoais, a comparação entre o Regulamento Geral sobre a Proteção de Dados da União Europeia (RGPD), aplicável em Portugal, e a Lei Geral de Proteção de Dados brasileira (LGPD), evidenciou que, embora existam semelhanças conceituais, o modelo europeu é mais completo, vinculante e tecnicamente maduro. O RGPD prevê obrigações específicas inclusive para atividades de investigação criminal, impondo limites rigorosos ao uso de dados em contextos policiais e judiciais. Já a LGPD brasileira, apesar de representar um avanço significativo no ordenamento nacional, apresenta lacunas e omissões quanto à sua aplicação no âmbito penal, o que dificulta a harmonização entre direitos fundamentais e necessidade de repressão eficaz.

Por fim, a análise demonstrou que Portugal possui políticas públicas de prevenção e combate ao cibercrime melhor estruturadas, com investimentos contínuos em formação de agentes, infraestrutura digital forense e campanhas educativas. O Brasil, embora tenha centros especializados em alguns estados e iniciativas isoladas, carece de um programa nacional integrado que articule prevenção, repressão, educação digital e cooperação internacional. Essa ausência de coordenação compromete a eficácia do enfrentamento sistêmico do cibercrime e revela uma lacuna significativa na formulação de uma política criminal digital moderna.

Capítulo 6 - Conclusão

6.1 A urgência de reformas legislativas

A presente investigação revelou, de forma sistemática e inquestionável, que o ordenamento jurídico brasileiro não apenas se mostra defasado, mas estruturalmente incompatível com a complexidade e a sofisticação do cibercrime contemporâneo. O sistema penal vigente, ainda lastreado em paradigmas analógicos e categorias dogmáticas tradicionais, é incapaz de oferecer respostas jurídicas eficazes, legítimas e proporcionais às ameaças emergentes do ambiente digital.

A inexistência de uma codificação penal coerente voltada especificamente aos delitos informáticos compromete a inteligibilidade do direito penal e enfraquece a sua função preventiva e repressiva. O atual modelo — fragmentado, disperso e lacunar — conduz a uma criminalização assistemática das condutas digitais, o que prejudica a segurança jurídica, favorece decisões judiciais contraditórias e impõe obstáculos relevantes à atuação do Ministério Público e das polícias judiciárias.

No plano processual, a ausência de regulamentação específica sobre a prova digital evidencia um cenário ainda mais preocupante. Questões cruciais como a cadeia de custódia eletrônica, a coleta de evidências em nuvem, o espelhamento forense de dispositivos, a interoperabilidade entre sistemas e a validade de dados obtidos por meios automatizados permanecem sem disciplina normativa clara. A consequência prática dessa omissão tem sido a proliferação de nulidades processuais, a ineficácia da persecução penal e, em muitos casos, a completa inviabilidade de responsabilização penal de agentes que operam no anonimato da rede.

Diante desse cenário, torna-se imperativo conceber uma reforma legislativa ampla, articulada e tecnicamente qualificada. A criação de um Código Penal Digital não deve ser vista como uma inovação simbólica, mas como instrumento de reorganização do sistema penal, capaz de integrar tipificações atualizadas, garantir coerência sistemática e estabelecer um marco normativo adequado à era digital. Esse novo código deve preservar os princípios constitucionais, mas avançar em direção a uma estrutura normativa adaptada às especificidades do ciberespaço.

Outro eixo essencial da reforma diz respeito à responsabilização penal de pessoas jurídicas, especialmente nos casos em que plataformas tecnológicas, empresas de infraestrutura digital e instituições financeiras contribuem, por ação ou omissão, para a ocorrência de crimes cibernéticos. A ausência de previsões claras sobre os deveres de controle, monitoramento e contenção de atividades ilícitas no âmbito corporativo favorece a impunidade e desestimula a autorregulação do setor privado.

As reformas legislativas devem, ainda, contemplar com precisão os novos riscos à soberania digital e à segurança nacional. A normatização de condutas como sabotagem eletrônica, espionagem cibernética, manipulação algorítmica de processos democráticos e ataques a infraestruturas críticas é urgente. Não se trata de mera atualização técnica, mas da proteção de bens jurídicos fundamentais que definem a integridade do Estado contemporâneo.

Por fim, o alinhamento do ordenamento jurídico interno aos compromissos internacionais assumidos pelo Brasil é condição inadiável. A adesão à Convenção de Budapeste, por si só, não assegura eficácia se não vier acompanhada da internalização de dispositivos compatíveis com os mecanismos de cooperação jurídica internacional, troca de informações em tempo real e harmonização procedimental com os demais países signatários.

Reformar a legislação penal e processual no campo do cibercrime não é apenas uma necessidade jurídica: é uma exigência institucional, ética e civilizatória. O Estado que insiste em operar com ferramentas do século passado para enfrentar crimes do século XXI transforma o seu sistema de justiça em um instrumento inócuo, disfuncional e, por vezes, violador das próprias garantias que pretende proteger.

6.2 Cooperação internacional: o papel da Convenção de Budapeste

A transnacionalidade inerente aos crimes cibernéticos tornou obsoleta qualquer tentativa de enfrentamento isolado por parte dos Estados. A territorialidade — fundamento clássico do direito penal — mostra-se insuficiente diante da arquitetura técnica da internet, cujas infrações extrapolam fronteiras em tempo real, fragmentando competências, ocultando autores e dificultando investigações. Nesse cenário, a cooperação jurídica internacional

assume papel central não apenas como instrumento auxiliar, mas como pilar estruturante de qualquer política criminal eficaz no século XXI.

A adesão do Brasil à Convenção de Budapeste, formalizada por meio do Decreto Legislativo nº 37/2021 e promulgada pelo Decreto nº 11.491/2023, representou um marco histórico para o sistema penal brasileiro. Mais do que um gesto de alinhamento político ao Conselho da Europa, essa adesão traduziu o reconhecimento oficial da incapacidade do ordenamento jurídico nacional em enfrentar, de forma autônoma, as ameaças cibernéticas que desafiam diariamente a soberania digital do Estado.

A Convenção de Budapeste, ao estabelecer um conjunto mínimo de infrações penais comuns, procedimentos harmonizados para coleta e preservação de provas digitais, e canais permanentes de assistência mútua entre autoridades competentes, promove uma racionalização imprescindível da cooperação internacional em matéria penal. No caso brasileiro, esse tratado obriga à implementação de mecanismos jurídicos que ainda não estão plenamente institucionalizados, como o acesso transfronteiriço a dados, a coleta em tempo real de informações de tráfego e a preservação expedita de conteúdos armazenados por terceiros.

A designação de um ponto de contato nacional, disponível 24 horas por dia, como previsto no artigo 35 da Convenção, é apenas a base técnica mínima exigida. O verdadeiro desafio reside na construção de uma cultura institucional de cooperação proativa, na qual os operadores do sistema de justiça estejam capacitados para agir com celeridade, segurança jurídica e interoperabilidade procedimental em cenários de criminalidade digital difusa e interconectada.

Importa ressaltar que o ingresso do Brasil na Convenção também impõe o dever de ajustar sua legislação penal e processual aos padrões internacionais de proteção de direitos fundamentais, evitando tanto o excesso repressivo quanto as omissões permissivas. Isso significa que o Estado brasileiro deve implementar reformas normativas que assegurem a proteção da privacidade, da integridade probatória e do contraditório, mesmo nos casos de compartilhamento internacional de dados, solicitação de interceptações ou apreensões em nuvem.

A participação ativa do Brasil em programas de capacitação técnica, pesquisas comparadas, fóruns multilaterais e projetos transnacionais de repressão ao cibercrime é outro desdobramento necessário dessa adesão. A cooperação internacional não pode ser limitada à troca pontual de informações ou à execução passiva de cartas rogatórias — ela exige engajamento estratégico, investimento institucional e projeção geopolítica. O Brasil, enquanto potência regional, tem o dever de ocupar posição de liderança no desenvolvimento de normas internacionais, protocolos técnicos e pactos multilaterais que definam os rumos da governança digital penal.

Assim, a Convenção de Budapeste deve ser compreendida não como um fim em si mesma, mas como o ponto de partida para a construção de um modelo brasileiro de cooperação penal internacional robusto, alinhado com os valores democráticos, comprometido com a proteção dos direitos humanos e tecnicamente preparado para atuar com eficácia em um ambiente criminal globalizado, volátil e sofisticado.

6.3 A transformação necessária: tecnologia e especialização

A persistente inadequação do sistema de justiça criminal frente às complexidades dos delitos cibernéticos transcende a problemática legislativa. Trata-se, na verdade, de um fenômeno institucional mais amplo, que exige uma verdadeira reengenharia funcional centrada em dois vetores complementares: a incorporação sistemática de tecnologias nos processos judiciais e investigativos, e a consolidação de uma cultura permanente de especialização técnica dos operadores jurídicos.

A tecnologia, no contexto do cibercrime, não é apenas um instrumento auxiliar — ela constitui o próprio cenário da infração, a fonte de evidência e o meio pelo qual o ilícito se perpetra e se oculta. Ignorar essa realidade equivale a comprometer, na origem, a eficácia da persecução penal. O modelo atual, baseado em procedimentos físicos e dogmáticas tradicionais, atua como um obstáculo estrutural à efetividade, à celeridade e à integridade das investigações e julgamentos no ambiente digital.

É urgente que o sistema de justiça seja dotado de infraestrutura tecnológica compatível com os desafios que enfrenta. Isso implica a digitalização completa dos autos processuais, a criação de protocolos padronizados de custódia eletrônica, o emprego de softwares forenses certificados, o uso de criptografia robusta na manipulação de provas digitais, a

integração com bases de dados nacionais e internacionais, e a utilização controlada de algoritmos para rastreamento de fluxos informacionais. Normas internacionais como a ISO/IEC 27037, que delineiam padrões para coleta e preservação de evidências digitais, devem ser internalizadas como referência obrigatória em qualquer procedimento probatório envolvendo delitos informáticos.

Entretanto, nenhuma inovação tecnológica terá impacto real se não for acompanhada da qualificação técnica dos profissionais que operam o sistema. A complexidade do cibercrime impõe que juízes, promotores, defensores, delegados e peritos sejam não apenas conhecedores do Direito, mas também versados nas dinâmicas técnicas do ciberespaço. O modelo de formação jurídica tradicional, centrado em dogmas analógicos e fórmulas processuais estanques, mostra-se claramente insuficiente diante da realidade digital.

A especialização, nesse contexto, deve deixar de ser episódica ou voluntária, para se tornar eixo estruturante da política institucional. Isso exige a criação de programas obrigatórios de formação continuada, certificações técnicas periódicas, avaliação de desempenho baseada em competência digital e participação ativa dos operadores jurídicos em fóruns internacionais de atualização legislativa e doutrinária.

Além da capacitação individual, é necessária a criação de unidades institucionais especializadas. Varas criminais digitais, promotorias cibernéticas e delegacias de crimes tecnológicos não podem mais figurar como projetos experimentais ou iniciativas regionais isoladas. Elas devem ser estabelecidas como estruturas permanentes, com orçamento próprio, equipe multidisciplinar e acesso prioritário a recursos tecnológicos de ponta. A centralização temática dessas unidades favorece a construção de precedentes jurisprudenciais coerentes, a qualificação da prova técnica e a uniformização de entendimentos judiciais — elementos fundamentais para restaurar a segurança jurídica no campo digital.

As polícias judiciárias carecem de reformulação técnica e administrativa. A atuação frente aos crimes digitais demanda conhecimentos que extrapolam a investigação tradicional: é preciso compreender arquitetura de redes, criptografia, engenharia reversa, rastreamento de ativos digitais e anonimização de dados. Sem a internalização dessas competências, a

persecução penal permanece ineficaz, dependente da sorte ou da colaboração fortuita de empresas privadas.

A transformação institucional que se impõe, portanto, não é gradual, mas estrutural. Ela exige planejamento de longo prazo, financiamento público robusto e, sobretudo, vontade política. Seus custos, embora significativos, são incomparavelmente inferiores às perdas que o país sofre com fraudes digitais, ataques a infraestruturas críticas, evasão de dados sensíveis e o fortalecimento de redes criminosas transnacionais operando sob a proteção da inércia estatal.

É chegada a hora de romper com a resistência histórica à inovação e de inaugurar uma nova cultura jurídica, ancorada em eficiência, transparência e responsabilidade técnica. A especialização e a tecnologia não são acessórios institucionais — são vetores de legitimidade democrática e instrumentos indispensáveis de proteção da ordem pública na era digital. Adiar essa transformação é perpetuar a disfunção; realizá-la é assumir, com maturidade institucional, o compromisso com um sistema de justiça contemporâneo, acessível e verdadeiramente eficaz.

6.4 Considerações finais

Esta dissertação não encerra um ciclo; ela inaugura uma ruptura. Diante de um cenário jurídico ancorado em estruturas analógicas do século passado, confrontado por ameaças digitais que avançam com a velocidade da luz e a volatilidade de um código em constante mutação, este trabalho apresenta-se como um gesto acadêmico de insurgência. Insurgência contra a obsolescência do direito penal clássico, contra a passividade institucional diante de um novo território criminal que desafia os marcos da territorialidade, da autoria e da materialidade.

O cibercrime não é uma anomalia do sistema penal: é o sintoma mais eloquente da falência de uma arquitetura jurídica que não acompanhou a transição civilizacional para a era digital. Ele representa a fronteira em que os códigos jurídicos encontram os códigos computacionais — e perdem. Não porque faltem leis, mas porque falta um novo paradigma. Um paradigma que não apenas reescreva o direito, mas reconceba sua função diante da reorganização informacional do poder, da violência e da economia no século XXI.

Neste contexto, a ausência de um Código Penal Digital, a precariedade da regulamentação da prova eletrônica, a inexistência de estruturas institucionais especializadas e a insuficiência da cooperação internacional não podem mais ser tratadas como deficiências técnicas ou omissões legislativas. São expressões de uma inadequação epistemológica profunda, que compromete a legitimidade do Estado na sua missão de proteger bens jurídicos essenciais e preservar a confiança pública na justiça.

Ao longo da pesquisa, buscou-se não apenas diagnosticar as lacunas do ordenamento jurídico brasileiro, mas também formular propostas capazes de restabelecer a coerência entre o aparato normativo e as exigências impostas por um mundo interligado por redes descentralizadas, inteligência artificial e estruturas criptográficas de difícil rastreamento. Essas propostas não aspiram a uma resposta definitiva — pois a mutabilidade tecnológica exige do direito uma postura de vigilância contínua e capacidade adaptativa. Trata-se de esboçar, com responsabilidade científica, um novo pacto normativo digital.

Reconhece-se, com clareza metodológica, os limites do presente estudo. Optou-se por uma abordagem jurídico-normativa, o que impediu o enfrentamento empírico de variáveis relevantes, como o perfil das vítimas, a atuação das plataformas digitais diante da cooperação penal, ou os impactos orçamentários da criação de estruturas especializadas. No entanto, essas ausências foram deliberadas — pois a ambição desta dissertação foi outra: colocar em tensão os próprios fundamentos do sistema jurídico vigente diante da lógica disruptiva da criminalidade digital.

O desafio que se impõe não é apenas legal. Ele é filosófico, institucional, político e cultural. Requer uma refundação da dogmática penal à luz dos princípios da rastreabilidade digital, da proteção algorítmica dos direitos fundamentais e da inteligência regulatória aplicada à tecnologia. Exige, sobretudo, um Estado digitalmente competente — não apenas do ponto de vista técnico, mas ético e democrático.

É nesse sentido que esta dissertação não oferece um desfecho, mas um chamado: à ciência jurídica para que abandone o conforto das fórmulas repetidas; ao legislador para que ouça a urgência silenciosa que emana dos vazios normativos; ao sistema de justiça para que cesse de operar no escuro técnico da ignorância digital; e à sociedade civil para que compreenda que o espaço virtual é também um espaço político, onde se decide a liberdade, a dignidade e a segurança de milhões.

Portanto, o que aqui se propõe não é uma conclusão. É uma convocação: para que o Direito Penal não seja apenas o último a chegar à era digital, mas que — uma vez desperto — tenha coragem de reconstruir-se como instrumento legítimo de justiça em uma sociedade conectada, fragmentada e radicalmente transformada.

Referências

Bechara, F. (2020). *Direito penal*. São Paulo: Saraiva.

Bechara, F. (2021). Criminalidade informática: desafios e reações. *Revista de Ciências Criminais*, 29(1), 33–59.

Brasil. (2012). *Lei nº 12.737, de 30 de novembro de 2012*. Diário Oficial da União. https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm

Brasil. (2014). *Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet)*. Diário Oficial da União https://www.planalto.gov.br/ccivil_03/_ato2011 2014/2014/lei/l12965.htm

Brasil. (2018). *Lei nº 13.709, de 14 de agosto de 2018 (LGPD)*. Diário Oficial da União. https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

Brasil. (2023). *Decreto nº 11.491, de 12 de abril de 2023*. Promulga a Convenção sobre o Crime Cibernético. Diário Oficial da União https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11491.htm

CNCS – Centro Nacional de Cibersegurança. (2019). *Estratégia Nacional de Segurança do Ciberespaço 2019–2023*. https://www.cncs.gov.pt/pt/estrategia-nacional/

Conselho da Europa. (2001). *Convenção sobre o Cibercrime*. Budapeste. Promulgada no Brasil pelo Decreto nº 11.491/2023. https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11491.htm

Court of Justice of the European Union (CJEU). (2014). *Digital Rights Ireland and Seitlinger and Others, C-293/12 and C-594/12, ECLI:EU:C:2014:238*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293

Dandurand, Y., & Munro, J. (2020). *Cybercrime jurisdiction: A global survey*. United Nations Office on Drugs and Crime.

European Union Agency for Cybersecurity – ENISA. (2023). *Threat Landscape 2023*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

Europol. (2024). *Internet Organised Crime Threat Assessment (IOCTA)*. https://www.europol.europa.eu/publications-documents/internet-organised-crime-threat-assessment-iocta-2024

Ferreira, P., & Lopes, R. (2021). *Prova digital e garantias processuais: tensões constitucionais*. Revista Luso-Brasileira de Direito, 12(4), 221–247.

Martins, A. (2021). *Responsabilidade penal corporativa em crimes digitais*. Coimbra: Imprensa Acadêmica.

Neves, M. (2020). *Direito digital: fundamentos e perspectivas*. São Paulo: Revista dos Tribunais.

OECD. (2021). *Principles for Digital Security Risk Management*. https://www.oecd.org

ONU – Organização das Nações Unidas. (2024). *Relatório Global sobre Crimes Cibernéticos*.

Ramalho, J. (2022a). *Delimitação da tipificação do stalking no ordenamento jurídico-penal português*. Revista Eletrónica de Estudios Penales y de la Seguridad, 10(1), 1–16. https://www.ejc-reeps.com/n-mero-actual-2

Ramalho, J. (2022b). *Prova digital: articulação entre o Código Processual Penal Português e a Lei do Cibercrime*. Revista Eletrônica de Direito Penal e Política Criminal, 10(2), 7–20. https://seer.ufrgs.br/index.php/redppc/article/view/125530

Ramalho, J., & Almeida, F. (2024). *Apreensão de correio eletrónico: os regimes do Código de Processo Penal e da Lei do Cibercrime*. Revista Jurídica Portucalense, 7, 1–15. https://revistas.rcaap.pt/juridica/article/view/34119

Ramalho, J. M. F. da S. (2024). *Recolha de prova em suporte eletrónico: os regimes do Código de Processo Penal e a Lei do Cibercrime*. Jornal Jurídico (J²), 7(1), 1–9. https://revistas.ponteditora.org/index.php/j2/article/view/787

Ramalho, J., & Ramalho, S. (2023). *Sextortion: caracterização dogmática e delimitação da imputação criminal em Portugal*. Revista Eletrônica de Direito Penal e Política Criminal, 11(1/2), 129–142. https://seer.ufrgs.br/index.php/redppc/article/view/130672

Santos, L. (2022). *A criminalidade informática e os desafios para a legislação penal*. Revista Brasileira de Direito Penal, 19(3), 78–101.

SeguraNet. (2024). *Campanhas de sensibilização de cidadania digital*. https://www.seguranet.pt/campanhas/ciberseguranca-nas-escolas

UNODC – United Nations Office on Drugs and Crime. (2022). *Cybercrime and the Law*. https://www.unodc.org/unodc/en/cybercrime/index.html