PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS

ESCOLA DE DIREITO, NEGÓCIOS E COMUNICAÇÃO

NÚCLEO DE PRÁTICA JURÍDICA

COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO

MONOGRAFIA JURÍDICA

CRIMES CIBERNÉTICOS E OS DESAFIOS DA INVESTIGAÇÃO CRIMINAL NO BRASIL

UMA ANÁLISE JURÍDICA E INSTITUCIONAL SOBRE A GOVERNANÇA E AS POLÍTICAS PÚBLICAS DE ENFRENTAMENTO AO CIBERCRIME

ORIENTANDO (A): RENAN OLIVEIRA ARAUJO SILVA

ORIENTADORA: PROFA: Ma. ÉVELYN CINTRA ARAÚJO

GOIÂNIA - GO
2026

RENAN OLIVEIRA ARAUJO SILVA

CRIMES CIBERNÉTICOS E OS DESAFIOS DA INVESTIGAÇÃO CRIMINAL NO BRASIL

UMA ANÁLISE JURÍDICA E INSTITUCIONAL SOBRE A GOVERNANÇA E AS POLÍTICAS PÚBLICAS DE ENFRENTAMENTO AO CIBERCRIME

Monografia jurídica apresentada à disciplina Trabalho de Curso II, da Escola de Direito, Negócios e Comunicação, Curso de Direito, da Pontifícia Universidade Católica de Goiás (PUCGOIÁS).
Prof.(a) Orientadora: Ma. Évelyn Cintra Araújo.

GOIÂNIA - GO
2026

RENAN OLIVEIRA ARAUJO SILVA

CRIMES CIBERNÉTICOS E OS DESAFIOS DA INVESTIGAÇÃO CRIMINAL NO BRASIL

UMA ANÁLISE JURÍDICA E INSTITUCIONAL SOBRE A GOVERNANÇA E AS POLÍTICAS PÚBLICAS DE ENFRENTAMENTO AO CIBERCRIME

Data da Defesa: _____ de _____ de _____

BANCA EXAMINADORA

_____

Orientador (a): Professora Ma. Évelyn Cintra Araújo. Nota

_____

Examinador (a) Convidado (a): Prof. (a): Titulação e Nome Completo Nota

Dedico este trabalho à minha família, à minha namorada e a todas as vítimas de crimes cibernéticos, cujas experiências evidenciam a importância do enfrentamento dessa realidade.

AGRADECIMENTOS

À Luisa, a pessoa que mais amo neste mundo e, sem dúvida, quem mais me compreende. Obrigado por estar ao meu lado em todos os momentos e por tornar essa caminhada mais leve.

Ao meu pai, Rodney, minha maior referência. Sua dedicação, competência e disposição em sempre ajudar são exemplos que levo para a vida. Se eu alcançar parte do que ele representa, já me considerarei bem-sucedido.

À minha mãe, Eneida, exemplo de trabalho, dedicação e entrega à família, cuja força e compromisso sempre foram fundamentais para minha formação.

Às minhas irmãs, pela convivência e pelos momentos compartilhados ao longo da vida.

Aos meus amigos, pela parceria e pelos momentos compartilhados durante essa jornada.

RESUMO

O presente trabalho analisou os crimes cibernéticos e os desafios enfrentados pela investigação criminal no Brasil, sob a perspectiva do Direito Penal e Processual Penal, buscando compreender a efetividade do sistema de justiça diante das transformações impostas pela sociedade da informação. Utilizou-se método dedutivo, com abordagem qualitativa e pesquisa bibliográfica e documental, a partir da análise de doutrina, legislação, jurisprudência e documentos técnicos. Inicialmente, examinou-se a evolução histórica da criminalidade digital, bem como seus conceitos, tipologias e impactos sociais, econômicos e jurídicos, evidenciando sua relação direta com o avanço tecnológico. Em seguida, analisou-se o marco jurídico brasileiro aplicável ao cibercrime, com destaque para a Lei nº 12.737/2012, o Marco Civil da Internet e a Lei Geral de Proteção de Dados, identificando avanços normativos, mas também limitações quanto à efetividade prática. Por fim, verificou-se que os principais entraves à investigação criminal não são apenas de natureza legislativa, mas sobretudo estruturais, técnicos e institucionais, envolvendo a volatilidade da prova digital, as dificuldades de cooperação internacional, o uso de técnicas de anonimização e as limitações dos órgãos de persecução penal. Concluiu-se que o enfrentamento da criminalidade cibernética exige não apenas o aprimoramento normativo, mas principalmente o fortalecimento institucional, a capacitação técnica e a adoção de políticas públicas integradas, capazes de assegurar a efetividade da persecução penal no ambiente digital.

Palavras-chave: crimes cibernéticos; investigação criminal; prova digital; persecução penal; cooperação internacional.

SUMÁRIO

INTRODUÇÃO

A presente pesquisa tem por objeto o estudo dos crimes cibernéticos e dos desafios enfrentados pelos órgãos de persecução criminal no Brasil, em especial pelas Polícias Judiciárias e pelo Ministério Público, analisando-os sob uma perspectiva jurídica e institucional. Observa-se que a atuação estatal não tem acompanhado, em igual medida, o avanço das tecnologias digitais, que ampliaram significativamente as possibilidades de comunicação e interação social, ao mesmo tempo em que viabilizaram novas formas de prática delitiva, marcadas pela transnacionalidade, pela sofisticação técnica e pela dificuldade de identificação dos agentes.

No plano jurídico, observa-se que o ordenamento brasileiro desenvolveu, de forma gradual, instrumentos normativos voltados ao enfrentamento do cibercrime, com destaque para a Lei nº 12.737/2012, o Marco Civil da Internet (Lei nº 12.965/2014) e a Lei Geral de Proteção de Dados (Lei nº 13.709/2018). Todavia, verificou-se que a existência desse arcabouço legislativo não é, por si só, suficiente para assegurar a efetividade da persecução penal, na medida em que os principais entraves à investigação criminal decorrem de fatores técnicos, operacionais e institucionais.

Nesse contexto, serão examinados como elementos centrais da problemática a volatilidade da prova digital, a necessidade de cooperação internacional, o uso de técnicas de anonimização e criptografia, bem como as limitações estruturais e a carência de capacitação técnica dos órgãos de persecução penal. Tais aspectos indicam que o enfrentamento do cibercrime exige não apenas atualização normativa, mas também o aperfeiçoamento das práticas investigativas, e o fortalecimento da governança institucional e a capacidade de atuação interagências.

A relevância do tema justifica-se tanto por sua atualidade quanto por seu impacto social, uma vez que os crimes cibernéticos atingem, de forma crescente, não apenas instituições públicas e privadas, mas também cidadãos comuns, expondo vulnerabilidades estruturais do sistema de justiça criminal. Além disso, trata-se de matéria de natureza interdisciplinar, envolvendo o Direito Penal, o Direito Processual Penal, o Direito Constitucional e o Direito Digital, em diálogo com áreas técnicas como a ciência de dados e a criminologia.

Diante desse cenário, surgem como problemas de pesquisa: a) se a evolução da criminalidade digital impõe a revisão dos modelos tradicionais de investigação

criminal; b) se o marco normativo brasileiro é suficiente para garantir a efetividade da persecução penal em crimes cibernéticos; c) quais são os principais entraves técnicos, probatórios e institucionais à investigação de delitos digitais no Brasil; e d) em que medida a ausência de integração entre os órgãos de persecução penal compromete a governança e a eficácia das políticas públicas de enfrentamento ao cibercrime.

Como hipóteses, parte-se da premissa de que a evolução da criminalidade digital acompanha o avanço tecnológico e exige a superação de modelos tradicionais de investigação; de que o arcabouço normativo brasileiro, embora relevante, não é suficiente para garantir a efetividade da persecução penal; de que a volatilidade da prova digital, o anonimato e a ausência de padronização técnica comprometem a cadeia de custódia e a confiabilidade probatória; de que os principais déficits no enfrentamento ao cibercrime são predominantemente de natureza estrutural e institucional; de que a baixa integração entre os órgãos de persecução penal compromete a eficiência investigativa; e, por fim, de que o fortalecimento de políticas públicas, da cooperação internacional e da capacitação técnica constituem condição essencial para o aprimoramento da investigação criminal no ambiente digital.

Para o desenvolvimento da pesquisa, adotar-se-á metodologia de natureza qualitativa, com abordagem bibliográfica e documental, baseada na análise de legislação, doutrina, jurisprudência e documentos técnicos relacionados ao tema. O método utilizado será o dedutivo, partindo-se de uma análise geral do fenômeno dos crimes cibernéticos na sociedade da informação para a investigação específica da realidade brasileira, seus entraves e suas práticas institucionais, buscando-se avaliar criticamente a efetividade do sistema investigativo e jurídico no enfrentamento da criminalidade digital.

Por fim, o trabalho será estruturado em três capítulos. No primeiro, analisar-se-á a evolução histórica da criminalidade digital, seus conceitos e tipologias. No segundo, cuidaremos do marco jurídico brasileiro aplicável aos crimes cibernéticos, identificando seus avanços e limitações. No terceiro, serão investigados os principais desafios da investigação criminal no Brasil, com enfoque na prova digital, na cooperação internacional, nas técnicas de anonimização e nas limitações estruturais dos órgãos de persecução penal.

CAPÍTULO 1 - CRIMES CIBERNÉTICOS NA SOCIEDADE DA INFORMAÇÃO

1.1 A EVOLUÇÃO HISTÓRICA DA CRIMINALIDADE DIGITAL

A compreensão da criminalidade digital exige uma análise histórica que permita identificar a forma como os avanços tecnológicos transformaram não apenas a vida social, mas também os mecanismos de violação de direitos, subversão de sistemas e prática de condutas ilícitas. O fenômeno não surgiu de maneira abrupta, ao contrário, desenvolveu-se de forma gradativa, acompanhando a consolidação da sociedade da informação e a crescente digitalização das interações humanas. Como destaca Patrícia Peck (2012), cada evolução tecnológica produz simultaneamente uma "evolução das vulnerabilidades", o que significa que novos instrumentos de comunicação e armazenamento de dados rapidamente se tornam novos ambientes para a atuação criminosa.

Inicialmente, durante as décadas de 1960 e 1970, o uso de computadores era restrito às universidades, empresas de grande porte e órgãos governamentais. Os chamados *computer crimes* dessa época não se assemelhavam ao cibercrime contemporâneo, tratavam-se, sobretudo, de manipulações internas de sistemas, fraudes contábeis, desvios realizados por funcionários com acesso autorizado ou atos de sabotagem de equipamentos de processamento. Como registram Britz (2009) e Clough (2010), não havia ainda um ambiente conectado em rede nem a possibilidade de ataques remotos. Por isso, os primeiros crimes digitais eram essencialmente internos e dependiam do acesso físico às máquinas.

O cenário se altera profundamente com o surgimento da internet e a expansão das redes de comunicação global nas décadas de 1980 e 1990. O avanço tecnológico rompeu barreiras físicas, expandiu a conectividade e, como observa Britz (2009, p. 4), "reduziu as barreiras tradicionais e, em verdade, serviu como um convite informal a visitantes desconhecidos". A autora descreve que muitos usuários perceberam tarde demais os riscos inerentes à exposição digital, tornando-se vítimas de furtos, perda de privacidade e de outros ilícitos, já outros permaneciam "ignorantes de sua vulnerabilidade" e prestes a sofrer danos. Essa observação torna evidente que a

criminalidade digital evolui na mesma velocidade da expansão dos meios tecnológicos e da adoção massiva da internet.

Com a popularização dos computadores pessoais, dos modems domésticos e dos primeiros serviços de e-mail e salas de bate-papo, surgem novas modalidades de condutas ilícitas cuja lógica se diferencia dos crimes tradicionais. Peck (2012) explica que a digitalização das interações sociais e econômicas abriu espaço para novos conflitos e novas formas de lesividade, sobretudo porque a estrutura do Direito tradicional não estava preparada para lidar com fenômenos como anonimato, territorialidade expandida, volatilidade de dados e velocidade de propagação das informações. Assim, ocorre uma transição histórica importante momento em que o crime deixa de ser apenas um ato cometido mediante contato físico ou presença no local e passa a ser praticado “à distância”, por meio do acesso indevido a sistemas, interceptação de dados e manipulação remota de informações.

É nesse contexto que autores como Britz (2009) e Clough (2010) consolidam a expressão *cybercrime*, entendida como o conjunto de atividades ilícitas praticadas com o uso de computadores, dispositivos eletrônicos e redes de informação. Para Britz, “o cibercrime envolve o uso de aparelhos eletrônicos para acessar, controlar, manipular ou utilizar dados para fins ilegais” (BRITZ, 2009, p. 16-17). Essa definição demonstra que o foco da criminalidade migra do objeto físico para o dado, que se torna o recurso mais valioso do ambiente digital. A informação, antes guardada em arquivos impressos ou pastas físicas, passa a estar armazenada em sistemas eletrônicos, tornando-se vulnerável a ataques remotos e clandestinos.

No Brasil, o desenvolvimento da criminalidade digital também ocorre de forma gradual. A partir dos anos 2000, com a ampliação do acesso à internet banda larga, surgem fenômenos como fraudes bancárias eletrônicas, clonagem de cartões, disseminação de vírus e, posteriormente, ataques sofisticados conhecidos como *phishing* e engenharia social. Emerson Wendt (2024), ao analisar a história do cibercrime no país, destaca que o avanço da digitalização bancária e comercial fez com que organizações criminosas migrassem parte de suas operações para o ambiente virtual, aproveitando-se da assimetria tecnológica entre criminosos altamente capacitados e usuários comuns com baixo conhecimento de segurança informática.

Os fatores que explicam o crescimento exponencial do crime cibernético podem ser sintetizados na observação de Clough (2010, p. 5), para quem três

elementos são determinantes: “a existência de criminosos motivados, a disponibilidade de oportunidades adequadas e a ausência de vigilância eficaz”. A internet, ao ampliar o alcance e a velocidade das comunicações, aumentou as oportunidades, em contrapartida a dificuldade estatal em fiscalizar ambientes virtuais complexos e a universalização do acesso digital cria motivação constante, seja por lucro, desafio intelectual, vingança, ideologia ou simplesmente pelo desejo de causar danos.

A partir de 2010, o cenário se torna ainda mais complexo. O cibercrime deixa de ser predominantemente individual e passa a incorporar estruturas organizadas, transnacionais e hierarquizadas, características típicas de organizações criminosas. A atuação de grupos especializados, como quadrilhas de *ransomware*, organizações voltadas para lavagem de dinheiro por criptomoedas, mercados ilícitos na *dark web* e redes de exploração de dados pessoais, evidencia que o crime digital não é mais uma atividade isolada, mas um fenômeno global conectado a fluxos financeiros, exploração de vulnerabilidades de software e cooperação criminosa internacional. É por isso que Wendt (2024) afirma que o cibercrime contemporâneo “transcende fronteiras, exige inteligência sofisticada e demanda cooperação institucional permanente”.

Outro marco importante é a ascensão dos ataques automatizados e do uso de inteligência artificial para a prática de ilícitos. Dispositivos de Internet das Coisas (IoT), assistentes virtuais, sistemas de automação residencial e algoritmos de recomendação ampliam o campo de vulnerabilidades e permitem a atuação criminosa em escala. Peck (2012) destaca que, na sociedade digital, “o tempo e a territorialidade são redefinidos”, de modo que a prática de um crime pode ocorrer em milissegundos e envolver múltiplos países simultaneamente. A velocidade e a ausência de limites geográficos fazem com que o Estado enfrente grandes dificuldades em identificar autores, coletar provas e estabelecer jurisdição.

Por fim, a evolução histórica do cibercrime evidencia que a criminalidade digital não é um fenômeno isolado ou circunstancial, mas uma consequência direta da integração tecnológica e da dependência crescente de sistemas informacionais. A cada avanço tecnológico corresponde, inevitavelmente, uma expansão das modalidades de ataque. A história demonstra, portanto, que o cibercrime acompanha o próprio desenvolvimento da sociedade da informação, exigindo do Estado, das instituições e dos usuários uma adaptação contínua e sofisticada para lidar com riscos cada vez mais complexos e transnacionais.

1.2 CONCEITO E TIPOLOGIAS DE CRIMES

A consolidação da sociedade da informação transformou profundamente a forma como os delitos são concebidos e praticados. No ambiente digital, condutas tradicionalmente realizadas no mundo físico passaram a ser executadas por meio de dispositivos eletrônicos conectados à internet, o que exige compreensão conceitual específica sobre os chamados crimes cibernéticos. De maneira geral, a doutrina aponta que esses delitos envolvem ações ilícitas praticadas com o uso, o direcionamento ou o alvo em sistemas informáticos, seja como instrumento, seja como ambiente de execução.

Nesse sentido, Patricia Peck (2012, p. 164) observa que “o crime eletrônico é, em princípio, um crime de meio, isto é, utiliza-se de um meio virtual. Não é um crime de fim, por natureza, ou seja, o crime cuja modalidade só ocorra em ambiente virtual, à exceção dos crimes cometidos por hackers, que de algum modo podem ser enquadrados na categoria de estelionato, extorsão, falsidade ideológica, fraude, entre outros”. A autora evidencia que, na maioria das situações, o ambiente digital não constitui o bem jurídico primário, mas sim o contexto instrumental que permite a prática delitiva, salvo em hipóteses específicas em que o próprio sistema ou dispositivo é o alvo.

Além disso, a internet frequentemente funciona como multiplicadora de oportunidades ilícitas, sobretudo pela facilidade de ocultação da identidade e pela desmaterialização dos rastros digitais. A mesma Patricia Peck (2012, p. 164) ressalta que “a maioria dos crimes cometidos na rede ocorre também no mundo real. A Internet surge apenas como um facilitador, principalmente pelo anonimato que proporciona”. Esse fenômeno demonstra que grande parte das tipologias criminais mantêm sua essência, mas ganham contornos próprios no ambiente virtual, ampliando a capacidade de execução e dificultando a identificação imediata dos responsáveis.

Assim, a doutrina e a prática policial passaram a classificar os crimes cibernéticos a partir de critérios funcionalmente úteis para a investigação, sendo um dos recortes mais aceitos aquele que diferencia condutas que têm como alvo dados ou sistemas informáticos, como invasões, interceptações e alterações de conteúdo, daquelas em que o computador ou a rede é utilizada como instrumento para atingir terceiros, como ocorre em fraudes, ameaças, extorsões e crimes contra a dignidade

sexual. Peck (2012, p. 164) sintetiza essa diversidade ao apontar que “os crimes eletrônicos ou cibernéticos têm modalidades distintas, dependendo do bem jurídico tutelado. Nesse sentido, pode-se citar crimes contra dados, como interceptação telefônica e de dados, e condutas como e-mail *bombing*, e-mails com vírus e *spam*”.

A partir dessa perspectiva, é possível identificar três grandes categorias analíticas: (a) crimes em que o computador é o meio para atingir um fim ilícito; (b) crimes em que o computador ou sistema é o próprio bem jurídico tutelado; e (c) crimes em que o ambiente digital é utilizado para potencializar práticas tradicionais. Essa divisão, embora simplificada, facilita a compreensão inicial das condutas e orienta a atuação investigativa, sobretudo diante do caráter multifacetado das práticas delitivas contemporâneas.

Entretanto, o crescimento expressivo de crimes cometidos em camadas mais profundas da rede, especialmente na *deep web* e na *dark web*, revela tipologias específicas que se desenvolvem exclusivamente nesse ambiente. Conforme Barreto e Santos (2019, p. 84), “ocorre que, por causa dessa possibilidade de privacidade irrestrita e de anonimato, mais uma vez a tecnologia é desvirtuada. Criminosos encontraram terreno fértil para o cometimento de ilícitos, principalmente para auferir lucros com venda de produtos ilegais e materiais contendo cenas de abuso sexual infantil”. A característica central dessa camada da internet é justamente a dificuldade de rastreabilidade, o que atrai agentes motivados por atividades de alto risco jurídico e moral.

Entre essas condutas, destaca-se especialmente o comércio de drogas sintéticas, cuja circulação é profundamente facilitada por mecanismos criptografados e canais de pagamento anônimos. Os mesmos autores observam que “o tráfico de drogas, principalmente as sintéticas, é um dos principais crimes cometidos através da internet, principalmente na deep web, cenário no qual prevalece a dificuldade da identificação da autoria, notadamente em razão do anonimato” (BARRETO; SANTOS, 2019, p. 88). Trata-se de crime tradicional que encontra no meio digital a possibilidade de ampliação de alcance, redução de riscos e expansão de mercados ilícitos.

Outro delito de extrema relevância, e que adquire dimensões agravadas no contexto digital, é o abuso e a exploração sexual de crianças e adolescentes. Conforme registram Barreto e Santos (2019, p. 92-94), “um dos crimes mais praticados nas redes da deep web é o abuso e a exploração sexual de crianças e adolescentes […] Na deep web, o terreno é vasto e fértil para a divulgação desse tipo

de material, que é produzido em várias partes do mundo, inclusive no Brasil". Essa tipologia apresenta enorme complexidade investigativa, pois envolve redes internacionais, armazenamento descentralizado, distribuição por canais criptografados e permanente reconfiguração de plataformas.

Em paralelo às condutas cometidas na internet profunda, observa-se também o crescimento de crimes tecnológicos ligados diretamente à violação ou manipulação de sistemas informáticos. A literatura especializada destaca que muitas infrações estão associadas à exploração de vulnerabilidades, técnicas de engenharia social, interceptações ilegais e uso de softwares maliciosos. Esses delitos exigem respostas específicas de capacitação e aprimoramento das unidades investigativas, como aponta Emerson Wendt ao mencionar que a padronização e o treinamento de equipes são essenciais para a atuação eficaz em contextos altamente tecnológicos, envolvendo "profissionais de *offensive security* na aquisição de sistemas e softwares para extração, mineração e análise de dados" (WENDT, 2024, p. 97).

A multiplicidade de tipologias demonstra que os crimes cibernéticos não constituem categoria homogênea. Pelo contrário, formam um espectro amplo que abrange desde atividades simples, como o envio de spam, até delitos organizados e transnacionais, como ataques de *ransomware* (sequestro de dados), espionagem industrial e venda de entorpecentes. Essa diversidade impõe dificuldades conceituais e metodológicas ao Estado, ao mesmo tempo em que exige estratégias diferenciadas para prevenção, investigação e responsabilização.

Ademais, o rápido avanço tecnológico evidencia que novas tipologias surgem a cada transformação no uso social da internet. Plataformas de comunicação, redes sociais, sistemas de pagamentos, ambientes virtuais descentralizados e dispositivos conectados ampliam constantemente as oportunidades de ação criminosa. Nesse cenário, a compreensão do conceito e das tipologias de crimes cibernéticos não pode ser estática, devendo acompanhar a evolução dos meios e das formas de interação digital.

Assim, o estudo das modalidades delitivas no ambiente virtual constitui etapa essencial para compreender os capítulos posteriores desta pesquisa, especialmente no que diz respeito aos desafios investigativos, às lacunas normativas e à atuação institucional. A definição conceitual e a identificação das principais tipologias fornecem o alicerce para análise aprofundada dos obstáculos enfrentados pelo poder público no

enfrentamento à criminalidade digital, bem como para a construção de políticas públicas integradas capazes de fortalecer a segurança cibernética no Brasil.

1.3 IMPACTOS SOCIAIS, ECONÔMICOS E JURÍDICOS DO CIBERCRIME

A sociedade da informação transformou profundamente a dinâmica social, econômica e jurídica contemporânea. Se antes os riscos estavam concentrados em ambientes físicos, hoje a hiperconectividade expõe indivíduos e instituições a ameaças que se propagam de forma instantânea e global. O ambiente digital ampliou a velocidade e a intensidade com que impactos se disseminam, criando novas formas de vulnerabilidade e exigindo estruturas de proteção mais robustas. Como observa Patricia Peck (2012, p. 42), “se, por um lado, é muito bom estar conectado, por outro o comportamento irracional de mercado afeta a todos, onde quer que estejam, de maneira nunca antes experimentada”. A autora demonstra que a amplitude dos efeitos sociais do cibercrime decorre justamente dessa interdependência global.

Do ponto de vista social, o crescimento dos delitos digitais agrava desigualdades e produz efeitos que ultrapassam o dano patrimonial. Peck (2012) enfatiza que a adoção de tecnologias avançadas cria novos grupos de exclusão, ao assinalar que a sociedade convergente aumenta a distância entre países desenvolvidos e em desenvolvimento devido ao analfabetismo digital, parcela significativa da população que não domina as ferramentas necessárias para lidar com riscos tecnológicos. Essa desigualdade se reflete na maior vulnerabilidade de usuários com menor escolaridade digital, frequentemente vítimas de golpes, *phishing*, fraudes e manipulações.

Além disso, o cibercrime repercute diretamente na percepção de segurança das pessoas. A facilidade de difusão de discursos de ódio, ataques contra a honra, vazamentos de dados pessoais, perseguições on-line e exploração sexual de crianças cria uma sensação permanente de insegurança. O ambiente digital, marcado por anonimato relativo, favorece comportamentos agressivos e dificulta a responsabilização. A literatura sobre dark web demonstra que a estrutura anônima dessas camadas da rede intensifica práticas ilícitas, como comércio ilegal, venda de

drogas sintéticas e circulação de material de abuso infantil, ampliando os impactos sociais e psicológicos sobre vítimas e familiares.

No campo econômico, as consequências do cibercrime assumem proporções bilionárias. A economia contemporânea depende da integridade dos dados e da continuidade operacional dos sistemas informáticos. Qualquer incidente, como *ransomware*, vazamento de informações, fraudes bancárias ou sabotagens, acarreta prejuízos severos para empresas e governos. A ISO/IEC 27002, por exemplo, destaca que a segurança da informação visa proteger os ativos informacionais para garantir a continuidade do negócio e minimizar riscos, maximizando os retornos e oportunidades econômicas (ISO/IEC 27002). Essa concepção demonstra que a informação é hoje um ativo estratégico fundamental.

A relevância econômica fica clara em episódios concretos da realidade brasileira. Em 2021, o Tribunal de Justiça do Rio Grande do Sul sofreu um ataque de *ransomware* que paralisou suas atividades por meses, interrompendo prazos, audiências, acesso a sistemas essenciais e gerando impactos financeiros e administrativos expressivos. O episódio mostrou como instituições públicas, mesmo com infraestrutura robusta, podem sofrer colapsos operacionais causados por grupos criminosos digitais. Tal evento evidencia de maneira empírica o potencial destrutivo do cibercrime, capaz de afetar a prestação jurisdicional e comprometer o funcionamento de todo um Poder Judiciário (G1, 2021).

Marcos Sêmola (2003) reforça a visão de que a informação possui valor jurídico e econômico que exige proteção técnica e conformidade legal. Para o autor, a segurança da informação se relaciona diretamente com a prevenção de prejuízos decorrentes de vazamentos, usos indevidos, danos a terceiros, fraudes e invasões. Nesse sentido, Patrícia Peck (2012) complementa ao destacar que a proteção jurídica da informação envolve evitar contingências legais associadas ao mau uso dos dados, ao vazamento de conteúdos confidenciais e às fraudes eletrônicas. Portanto, o impacto econômico não se limita à perda financeira imediata, mas também à reputação, à confiabilidade e aos passivos regulatórios.

Os prejuízos econômicos atingem igualmente o usuário comum, que frequentemente é o maior lesado em situações de insegurança digital. A autora alerta que, ao ser exposto a vírus ou a operações fraudulentas, o cidadão pode sofrer danos diretos e indiretos que se estendem por longo prazo (PECK, 2012). A soma dessas

perdas individuais gera impacto macroeconômico, reduzindo a confiança nas transações digitais e afetando setores inteiros da economia.

No plano jurídico, o cibercrime desafia profundamente os modelos tradicionais de regulação e aplicação da lei. A globalização das infrações demanda mudança de paradigma na interpretação das normas. Em uma de suas análises mais relevantes, Peck (2012, p. 43) afirma que “a globalização da economia e da sociedade exige a globalização do pensamento jurídico, de modo a encontrar mecanismos de aplicação de normas que possam extrapolar os princípios da territorialidade”. Esse trecho evidencia que o Direito Penal e o Direito Comercial devem dialogar com contextos transnacionais, especialmente em temas como cooperação internacional, coleta de provas, responsabilidade de provedores e jurisdição.

Os impactos jurídicos também incluem a necessidade de proteger direitos fundamentais no ambiente digital. Questões como privacidade, anonimato, liberdade de expressão e proteção de dados tornam-se centrais. Nesse sentido, o direito à privacidade atua como limite natural ao direito à informação, enquanto o anonimato pode dificultar mecanismos de segurança e investigação por parte de órgãos policiais. Esse conflito demonstra a complexidade do equilíbrio entre garantias individuais e efetividade da persecução penal.

No âmbito empresarial, os impactos jurídicos do cibercrime se manifestam em litígios envolvendo propriedade intelectual, concorrência desleal, dano moral, quebra de sigilo e responsabilidade civil. A intensificação desses conflitos acompanha a evolução da tecnologia. A visibilidade ampliada e a facilidade de circulação de dados criam riscos adicionais, pois, "a possibilidade de visibilidade do mundo atual traz também os riscos inerentes à acessibilidade, tais como segurança da informação, concorrência desleal, plágio, sabotagem por hacker, entre outros" (PECK, 2012, p. 46). Dessa forma, a incidência jurídica do cibercrime se expande tanto no âmbito penal quanto no civil e no empresarial.

Por fim, a informação, entendida como ativo crítico, compõe elemento central na governança jurídica das organizações. Sêmola (2003, p. 9) afirma que “a informação representa a inteligência competitiva dos negócios e é reconhecida como ativo crítico para continuidade operacional e saúde da empresa”. Dessa forma, qualquer incidente cibernético gera repercussões contratuais, administrativas e processuais, o que demonstra que os impactos jurídicos extrapolam a esfera criminal e alcançam toda a complexidade do ambiente regulatório contemporâneo

CAPÍTULO 2 - MARCO JURÍDICO BRASILEIRO SOBRE CRIMES CIBERNÉTICOS

2.1 LEI Nº 12.737/2012 (LEI CAROLINA DIECKMANN)

Em 2012, a atriz Carolina Dieckmann foi vítima da invasão de seu computador pessoal, tendo imagens íntimas divulgadas na internet sem sua autorização, o que gerou grande repercussão nacional e evidenciou a fragilidade da legislação brasileira diante de crimes cibernéticos (O GLOBO, 2012). Em resposta a esse cenário, foi sancionada a Lei nº 12.737, de 30 de novembro de 2012, conhecida como Lei Carolina Dieckmann, que representa o primeiro marco legislativo brasileiro voltado especificamente à tipificação de condutas praticadas mediante utilização de dispositivos informáticos. Sua promulgação inseriu no Código Penal o art. 154-A, criminalizando a invasão de dispositivo informático alheio, além de promover alterações pontuais em outros dispositivos legais.

A aprovação da norma ocorreu em um contexto de forte comoção social e intensa cobertura midiática. Conforme analisa Wendt (2023, p. 139), a imprensa exerceu papel relevante na construção da percepção social acerca da necessidade urgente de tipificação penal, o que contribuiu para a rápida tramitação e aprovação do projeto de lei, com conceitos amplos e pouco amadurecidos do ponto de vista técnico. Esse cenário ajuda a explicar determinadas fragilidades identificadas posteriormente pela doutrina.

Sob o aspecto dogmático, é importante reconhecer que muitos crimes praticados no ambiente digital não configuram delitos absolutamente novos, mas formas de execução virtual de condutas já conhecidas pelo Direito Penal tradicional. Nesse sentido, Patricia Peck (2012, p. 164) afirma que “o crime eletrônico é, em princípio, um crime de meio, isto é, utiliza-se de um meio virtual. Não é um crime de fim, por natureza”.

A Lei nº 12.737/2012 buscou suprir a lacuna existente quanto à invasão de dispositivos informáticos, especialmente diante da crescente prática de obtenção indevida de dados pessoais, senhas e informações sensíveis. O art. 154-A passou a prever como crime a invasão de dispositivo informático alheio, conectado ou não à

rede de computadores, mediante violação indevida de mecanismo de segurança, com o fim de obter, adulterar ou destruir dados ou informações.

Contudo, desde sua origem, o tipo penal foi alvo de críticas relevantes. Barreto, Kufa e Silva (2021, p. 131) destacam que a expressão “mediante violação indevida de mecanismo de segurança” possui natureza normativa e apresenta inconvenientes interpretativos, por depender de valoração fático-jurídica no caso concreto. Tal abertura conceitual pode gerar insegurança jurídica e divergências jurisprudenciais.

No mesmo sentido, os autores sustentam que o requisito de ausência de autorização expressa ou tácita do titular do dispositivo revela impropriedade técnica, sobretudo porque grande parte dos cibercrimes decorre de técnicas de engenharia social, nas quais o agente se vale do desconhecimento tecnológico da vítima (BARRETO; KUFA; SILVA, 2021, p. 133). Nesses casos, a análise da “autorização” torna-se complexa, podendo comprometer a adequada subsunção da conduta ao tipo penal.

Outra crítica relevante recai sobre o elemento subjetivo específico do tipo. Conforme observam Barreto, Kufa e Silva (2021, p. 132), a exigência de finalidade voltada a obter, adulterar ou destruir dados não contempla todas as modalidades de ataque atualmente difundidas, como ocorre nos casos de ransomware, em que os dados são tornados indisponíveis sem necessariamente serem destruídos ou alterados. Essa limitação demonstra que o legislador não alcançou integralmente a complexidade das condutas digitais contemporâneas.

No tocante à sanção originalmente prevista, a redação inicial do art. 154-A estabelecia pena de detenção de três meses a um ano, além de multa. A doutrina criticou a desproporcionalidade da reprimenda, considerada demasiadamente branda diante da gravidade potencial das condutas (BARRETO; KUFA; SILVA, 2021, p. 134). A baixa pena abstratamente cominada, além de dificultar medidas cautelares mais severas, esvaziava, na prática, o caráter dissuasório da norma.

Além disso, verificou-se ausência de diferenciação normativa entre condutas de menor e maior gravidade. Wendt (2023, p. 138) aponta que o mesmo tipo penal pode ser aplicado tanto a situações simples quanto a fatos complexos, sem distinção relevante no tratamento sancionatório. Tal uniformização compromete a individualização da pena e revela deficiência na técnica legislativa.

Em 2021, a Lei nº 14.155 promoveu alterações significativas no art. 154-A, ampliando as penas e ajustando sua redação. Ainda assim, conforme destaca Wendt (2023, p. 137), mesmo após as modificações, a pena privativa de liberdade não é percebida pelos policiais como plenamente efetiva no enfrentamento da criminalidade cibernética. Isso demonstra que o problema transcende a mera elevação de pena, envolvendo também questões estruturais da investigação e da persecução penal.

A complexidade de legislar em matéria digital já havia sido advertida por Patricia Peck (2012, p. 163), ao afirmar que “legislar sobre a matéria de crimes na era Digital é extremamente difícil e delicado. Isso porque, sem a devida redação do novo tipo penal, corre-se o risco de se acabar punindo o inocente”.

A advertência é particularmente pertinente no contexto da Lei nº 12.737/2012, cuja redação inicial revelou conceitos abertos e dependentes de interpretação, exigindo constante amadurecimento doutrinário e jurisprudencial.

Por fim, a evolução legislativa brasileira pode ser compreendida à luz dos estágios de amadurecimento normativo propostos pela autora, segundo os quais o primeiro estágio consiste na criação de tipos penais específicos para as novas condutas digitais. Não por outro motivo afirma-se que o Brasil ingressou recentemente nesse primeiro estágio (PECK, 2012, p. 167), sendo a Lei Carolina Dieckmann expressão desse momento inicial de estruturação da tutela penal no ambiente virtual.

Dessa forma, a Lei nº 12.737/2012 deve ser entendida como marco inaugural da criminalização específica da invasão de dispositivos informáticos no Brasil. Embora tenha representado avanço significativo ao preencher lacuna normativa relevante, apresentou limitações técnicas e estruturais que demandaram posteriores ajustes legislativos e continuam a suscitar debates acerca da efetividade da tutela penal no enfrentamento dos crimes cibernéticos.

2.2 MARCO CIVIL DA INTERNET (LEI Nº 12.965/2014)

A promulgação da Lei nº 12.965/2014, conhecida como Marco Civil da Internet (MCI), representou um marco estruturante na disciplina jurídica do ambiente digital brasileiro. Diferentemente da Lei nº 12.737/2012, de natureza eminentemente penal,

o Marco Civil assumiu caráter principiológico, estabelecendo direitos, garantias e deveres para o uso da Internet no país.

O Marco Civil representa uma tentativa de trazer de forma pioneira para a tutela judicial direitos fundamentais como a intimidade e a liberdade de expressão. A norma, portanto, não se limita a organizar tecnicamente a rede, mas busca concretizar direitos fundamentais no ambiente digital.

Em razão de sua abrangência normativa, o diploma ficou conhecido como “Constituição da Internet”, pois objetiva estabelecer as regras gerais para a utilização da rede no Brasil (MPF, 2013, p. 158). Contudo, como observa Gonçalves (2014, p. 8), quem efetivamente estabelece princípios e direitos fundamentais é a Constituição Federal, sendo o Marco Civil uma legislação infraconstitucional destinada a regulamentar e concretizar tais garantias no plano digital.

Nessa perspectiva, o MCI deve ser interpretado à luz dos direitos humanos, cuja natureza é marcada pela inderrogabilidade, inalienabilidade, interdependência e imprescritibilidade (GONÇALVES, 2014, p. 46). Assim, qualquer interpretação da norma deve respeitar a centralidade da dignidade da pessoa humana e a proteção integral das garantias fundamentais.

2.2.1 Liberdade de expressão e proteção da intimidade

Um dos principais desafios enfrentados pelo Marco Civil é o equilíbrio entre liberdade de expressão e direito à intimidade. O ambiente digital ampliou o alcance da manifestação do pensamento, mas também intensificou violações à honra, à imagem e à privacidade.

Conforme destaca o MPF, o direito à intimidade somente pode ser compreendido quando conciliado com as diversas dimensões da liberdade de expressão, seja como direito individual, como direito de acesso à informação ou como liberdade comercial relacionada à prestação de serviços digitais (MPF, 2013, p. 162). Essa visão evidencia que nenhum desses direitos possui caráter absoluto, devendo coexistir de maneira harmônica.

2.2.2 Neutralidade de rede e inclusão digital

A neutralidade de rede constitui outro pilar do Marco Civil. O princípio determina que os provedores de conexão devem tratar os dados de forma isonômica, sem discriminação por conteúdo, aplicação ou origem.

Contudo, a neutralidade não pode ser compreendida isoladamente. Gonçalves (2014, p. 58) ressalta que “a neutralidade só pode ser relevante se entrelaçada a outros princípios e valores que valorizem a inclusão digital, a busca da igualdade, a democracia e, por fim, a dignidade da pessoa humana”. Dessa forma, o princípio deve funcionar como instrumento de promoção da igualdade material e ampliação do acesso à informação.

Apesar de o acesso à Internet ter sido reconhecido como essencial ao exercício da cidadania, Gonçalves (2014, p. 41) observa que a legislação não solucionou integralmente as práticas de exclusão digital decorrentes de fatores econômicos, sociais e culturais. Isso demonstra que a efetividade do Marco Civil depende de políticas públicas estruturantes, sob pena de permanecer restrito ao plano formal.

2.2.3 Guarda de registros e investigação criminal

No âmbito investigativo, o Marco Civil desempenha papel fundamental ao disciplinar a guarda de registros de conexão e de acesso a aplicações.

O Ministério Público Federal, em seu Roteiro de atuação sobre crimes cibernéticos, enfatiza que as dificuldades investigativas são significativas, uma vez que o chamado “domicílio digital” pode ser facilmente alterado e envolve complexidades técnicas que exigem cooperação institucional e compartilhamento de informações (MPF, 2013, p. 165). Diante desse cenário, o MCI estabeleceu a obrigação de guarda de registros por período determinado, além de prever a possibilidade de requisição de dados cadastrais pelas autoridades competentes.

Nesse sentido, destaca-se que cabe ao Marco Civil viabilizar a obtenção de dados necessários à investigação, permitindo ao Ministério Público requisitar dados cadastrais e impondo às prestadoras o dever de conservação de registros por prazo razoável (MPF, 2013, p. 165).

Todavia, o acesso a tais dados deve observar critérios de proporcionalidade. Conforme leciona Gonçalves (2014, p. 108), “a busca pelos dados de registros deve ser a última solução numa investigação”. A obtenção de registros, portanto, deve ocorrer de forma subsidiária, preservando-se o direito à privacidade e o devido processo legal.

2.2.4 Marco Civil como etapa de consolidação normativa

O Marco Civil da Internet integra um processo gradual de amadurecimento do ordenamento jurídico brasileiro diante das transformações tecnológicas. Ao regulamentar princípios constitucionais no ambiente digital, a lei conferiu maior segurança jurídica às relações virtuais, disciplinando temas como neutralidade de rede, responsabilidade de provedores e guarda de registros.

Sua relevância reside na tentativa de equilibrar inovação tecnológica, proteção de direitos fundamentais e eficiência investigativa. Ainda assim, a consolidação plena de seus objetivos depende de interpretação jurisprudencial consistente, atuação institucional coordenada e políticas públicas voltadas à inclusão digital.

Em síntese, o Marco Civil da Internet representa instrumento normativo essencial para a organização jurídica do ciberespaço brasileiro. Ao mesmo tempo em que reforça a centralidade dos direitos fundamentais, estabelece mecanismos que permitem a responsabilização e a investigação de ilícitos, mantendo o necessário equilíbrio entre liberdade e segurança no ambiente digital.

2.3 LEI GERAL DE PROTEÇÃO DE DADOS (LEI Nº 13.709/2018)

A promulgação da Lei nº 13.709/2018, Lei Geral de Proteção de Dados Pessoais (LGPD), representa um marco estruturante na consolidação do Direito Digital brasileiro. Diferentemente das legislações anteriores, voltadas à tipificação penal de condutas específicas ou à regulamentação geral do uso da Internet, a LGPD estabelece um regime jurídico sistemático destinado à disciplina do tratamento de dados pessoais, impondo deveres aos agentes de tratamento e assegurando direitos aos titulares. Trata-se de diploma normativo que densifica o direito fundamental à privacidade e à autodeterminação informativa, posteriormente reconhecido de forma expressa no texto constitucional.

Na sociedade da informação, os dados assumiram posição central no modelo econômico contemporâneo. Como destaca Patricia Peck (2012, p. 53), “suas informações, em última análise, são um ativo e, portanto, de sua propriedade, e merecem proteção”. A informação deixa de ser mero elemento acessório e passa a

constituir ativo estratégico, tanto para indivíduos quanto para organizações. Nesse cenário, a autora observa que o grande paradigma atual não está na discussão abstrata sobre a necessidade de proteção da privacidade, que é inequívoca, mas no fato de que a informação se transformou na riqueza do século XXI e na própria moeda de pagamento nas relações digitais (PECK, 2012, p. 53).

Antes da promulgação da Lei Geral de Proteção de Dados, a doutrina já apontava a ausência de regras específicas que delimitassem, de maneira clara, o tempo máximo de utilização dos dados pessoais pelas empresas ou que vinculassem rigidamente as finalidades de tratamento às hipóteses de coleta. Nesse contexto, Patrícia Peck observava que o ordenamento jurídico brasileiro apresentava lacunas relevantes quanto à disciplina do tratamento de dados pessoais (PECK, 2012, p. 53). Esse cenário de insuficiência normativa somente viria a ser significativamente alterado com a edição da LGPD, que passou a estabelecer parâmetros objetivos para a coleta, o armazenamento, o compartilhamento e a eliminação de dados pessoais, reforçando a segurança jurídica e a proteção dos direitos fundamentais.

A proteção de dados deve ser compreendida também a partir dos interesses jurídicos tutelados no ambiente digital. Conforme ressalta Wendt (2023, p. 142), é necessário identificar os interesses jurídicos a serem protegidos em relação aos cibercrimes, permitindo adequada tipificação das condutas ilícitas, os quais podem ser extraídos dos pilares da segurança da informação. No mesmo sentido, Barreto, Kufa e Silva (2021, p. 83) afirmam que tais interesses devem ser resguardados tanto por medidas preventivas quanto por mecanismos repressivos. À míngua da aprovação de uma LGPD Penal e mesmo em face da natureza predominantemente administrativa e civil, ela dialoga diretamente com esses pilares técnicos, ao exigir a adoção de medidas capazes de garantir proteção efetiva aos dados pessoais.

Para que se alcance uma comunicação de dados fidedigna, devem ser observados requisitos como autenticação, autorização, não repúdio, integridade, confidencialidade e disponibilidade (BARRETO; KUFA; SILVA, 2021, p. 84-85). Esses elementos estruturam a segurança da informação e fundamentam tecnicamente as obrigações impostas pela LGPD. Entre tais pilares, a confidencialidade assume especial relevância, pois “reside no resguardo da informação sigilosa, impedindo seu conhecimento por terceiros não autorizados” (BARRETO; KUFA; SILVA, 2021, p. 89). A exigência legal de adoção de medidas técnicas e administrativas aptas a proteger

os dados pessoais contra acessos não autorizados evidencia a incorporação desses conceitos ao plano normativo.

A evolução legislativa brasileira demonstra que a proteção da intimidade no ambiente digital foi construída de forma gradual. Antes mesmo da LGPD, o Marco Civil da Internet já previa mecanismos específicos de tutela, como a possibilidade de notificação para remoção de conteúdos íntimos divulgados sem consentimento, nos termos do art. 21 da Lei nº 12.965/2014. Ainda assim, tais medidas possuíam caráter pontual e não configuravam um sistema abrangente de proteção de dados pessoais.

A construção normativa não esteve isenta de críticas. Wendt (2023, p. 137) aponta que inúmeras considerações foram feitas quanto à abertura conceitual existente em determinados diplomas legais, gerando expectativa de melhor redação dos dispositivos normativos. A observação revela desafio igualmente presente na LGPD, que contém conceitos jurídicos indeterminados, como legítimo interesse e medidas de segurança adequadas, cuja interpretação exige atuação regulamentar da Autoridade Nacional de Proteção de Dados e consolidação jurisprudencial.

A experiência legislativa anterior, especialmente no âmbito penal, reforça a centralidade da proteção de conteúdos sensíveis. Wendt (2023, p. 136) observa que, na legislação penal, a pena é majorada quando a invasão resulta na obtenção de comunicações eletrônicas privadas ou informações sigilosas, demonstrando que o ordenamento jurídico confere tratamento mais rigoroso às violações que atingem o núcleo da intimidade. Embora a LGPD não estabeleça sanções penais, mas administrativas e civis, sua lógica de proteção reforçada aos dados sensíveis mantém coerência com essa evolução normativa.

A LGPD também deve ser interpretada de forma sistemática, em consonância com os demais princípios do direito e normas vigentes sobre privacidade, proteção patrimonial, sigilo profissional e direitos do consumidor. Conforme ressalta Peck (2012, p. 108), cabe às empresas proteger as bases de dados de seus clientes, enquanto ao Estado compete, por meio de seu poder de polícia, proteger os usuários da Internet de modo geral. Essa perspectiva evidencia que a proteção de dados não é responsabilidade exclusiva do setor privado, mas resultado de atuação conjunta entre agentes econômicos e poder público.

Nesse contexto, a LGPD introduz modelo preventivo de proteção, impondo deveres de transparência, segurança e responsabilização aos agentes de tratamento. A lógica da governança de dados exige políticas internas, registro de operações,

avaliação de riscos e adoção de medidas técnicas adequadas. A proteção deixa de ser meramente reativa para assumir caráter estrutural, integrando a estratégia institucional das organizações.

Apesar de seu avanço, a efetividade da LGPD depende da consolidação de uma cultura de proteção de dados, da atuação fiscalizatória da Autoridade Nacional de Proteção de Dados e da harmonização entre inovação tecnológica e direitos fundamentais. A mera existência de norma não é suficiente para garantir proteção efetiva; é indispensável interpretação coerente, aplicação proporcional de sanções e investimento contínuo em segurança da informação.

Em síntese, a Lei Geral de Proteção de Dados consolida no ordenamento jurídico brasileiro um modelo normativo voltado à tutela estruturada da informação pessoal na sociedade digital. Ao reconhecer os dados como ativos sensíveis e ao estabelecer deveres preventivos de segurança, transparência e responsabilidade, a LGPD reafirma a centralidade da dignidade da pessoa humana no ambiente informacional, ao mesmo tempo em que impõe desafios interpretativos e operacionais que demandam constante aperfeiçoamento institucional e legislativo.

2.4 AVANÇOS, LACUNAS E DESAFIOS LEGISLATIVOS

A evolução da sociedade digital provocou profundas transformações nas relações sociais, econômicas e jurídicas, exigindo do Direito respostas capazes de acompanhar o desenvolvimento tecnológico e os novos riscos decorrentes do ambiente virtual. Nesse contexto, o ordenamento jurídico brasileiro passou a construir, gradativamente, um conjunto normativo voltado à regulação das atividades realizadas na Internet, especialmente no que diz respeito à proteção de dados, à responsabilização por ilícitos digitais e à investigação de crimes cibernéticos. Entretanto, embora tenham sido observados avanços significativos, persistem diversas lacunas e desafios legislativos que dificultam a plena efetividade das normas existentes.

A própria dinâmica tecnológica constitui um dos principais fatores que influenciam a elaboração e a aplicação das normas jurídicas no ambiente digital. O Direito, historicamente, sempre buscou adaptar-se às mudanças sociais e estruturais

da sociedade, acompanhando a evolução das formas de interação humana e das atividades econômicas. Nesse sentido, a adaptação às novas realidades tecnológicas não representa uma ruptura, mas sim a continuidade do processo evolutivo do próprio ordenamento jurídico (PECK, 2012, p. 45). Contudo, a velocidade das inovações tecnológicas frequentemente supera a capacidade de resposta do legislador, o que gera uma constante defasagem entre a realidade social e a regulamentação jurídica.

Nesse contexto, destaca-se que a própria estrutura normativa do Direito Digital precisa assumir características distintas das legislações tradicionais. Como afirma Patricia Peck (2012, p. 47), “no Direito Digital prevalecem os princípios em relação às regras, pois o ritmo de evolução tecnológica será sempre mais veloz que o da atividade legislativa”. Dessa forma, a legislação voltada ao ambiente digital tende a privilegiar princípios gerais e diretrizes amplas, capazes de se adaptar a novas tecnologias e situações jurídicas que surgem constantemente.

Outro aspecto relevante refere-se à própria natureza do ambiente virtual, que apresenta características distintas das relações jurídicas tradicionais. O ciberespaço constitui um ambiente globalizado, no qual indivíduos realizam transações, trocam informações e estabelecem relações jurídicas sem as limitações territoriais características do mundo físico. Nesse sentido, Barreto, Kufa e Mesquita Silva (2021, p. 70) observam que “muito da dificuldade encontrada no combate ao cibercrime advém da própria natureza do meio onde ocorre uma parte dos (ou todos os) atos executórios do delito, no caso o ciberespaço. Este pode ser conceituado como ‘o espaço indefinido onde os indivíduos transacionam e se comunicam’. Ou, ainda, ‘o lugar entre os lugares’”.

Essa característica do ambiente digital torna significativamente mais complexa a aplicação das normas jurídicas, sobretudo no que se refere à identificação dos autores de crimes, à coleta de provas digitais e à definição da competência jurisdicional para processamento das infrações.

Apesar dessas dificuldades, o ordenamento jurídico brasileiro apresentou avanços importantes na última década, especialmente com a criação de legislações voltadas à regulamentação da Internet e à proteção de direitos fundamentais no ambiente digital. A Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, introduziu a tipificação penal da invasão de dispositivos informáticos. Posteriormente, o Marco Civil da Internet (Lei nº 12.965/2014) estabeleceu princípios, garantias e direitos fundamentais para o uso da rede no Brasil, enquanto a Lei Geral de Proteção

de Dados (Lei nº 13.709/2018) instituiu um regime jurídico específico para a proteção de dados pessoais.

Essas normas representam importantes avanços no desenvolvimento do Direito Digital no país, demonstrando a tentativa do Estado brasileiro de construir um arcabouço jurídico capaz de lidar com as complexidades da sociedade da informação. Entretanto, a elaboração dessas leis ocorre em um contexto marcado por rápidas transformações tecnológicas e sociais. Como observa Emerson Wendt (2023, p. 115), a comunicação baseada em dados e informações circulando na Internet gera expectativas tanto cognitivas quanto normativas, especialmente porque a própria rede foi concebida sob uma lógica de liberdade e descentralização. Assim, a discussão contemporânea não gira mais em torno da possibilidade de regulação jurídica da Internet, mas sim acerca da forma pela qual essa regulação deve ocorrer.

Além disso, a própria estrutura global da Internet torna insuficientes soluções puramente nacionais para problemas que frequentemente ultrapassam fronteiras territoriais. Nesse cenário, a cooperação internacional assume papel essencial na investigação e repressão de crimes cibernéticos. Conforme destacam Barreto, Kufa e Mesquita Silva (2021, p. 121), “não é demais repisar que, precisamente no tocante ao cibercrime, obstaculizar a cooperação internacional é dar azo à criação de paraísos de cibercriminosos, a exemplo do que acontece com os paraísos fiscais.

A cooperação internacional, entretanto, envolve desafios institucionais e estruturais significativos. Nesse sentido, Hufnagel, Harfield e Bronitt destacam que:

> [...] o funcionamento eficaz da cooperação policial e judicial exige muito mais do que celebração de acordos estabelecendo procedimentos, organizando agências especiais e destinando recursos. Exige também o conhecimento e a imersão nos fundamentos das estruturas e culturas dos sistemas penais estrangeiros envolvidos. Além disso, é necessário saber como as coisas funcionam de fato na prática. E há, também, a necessidade de investimentos na formação e capacitação de policiais e servidores judiciais que estão regularmente chamados a cooperar. (HUFNAGEL; HARFIELD; BRONITT, 2012, p. 12).

Esse cenário demonstra que o enfrentamento da criminalidade cibernética exige não apenas legislação adequada, mas também mecanismos institucionais eficazes de cooperação internacional e capacitação profissional.

Outro desafio relevante diz respeito à própria capacidade institucional do Estado para lidar com as novas formas de criminalidade digital. O desenvolvimento constante de novas tecnologias amplia significativamente o potencial delitivo

associado ao ambiente virtual, exigindo atualização permanente das estruturas investigativas e dos profissionais responsáveis pela repressão desses crimes. Contudo, a resposta do aparato estatal muitas vezes se mostra insuficiente diante da complexidade das infrações digitais e da velocidade das transformações tecnológicas.

Nesse contexto, a capacitação técnica de agentes públicos torna-se elemento essencial para o enfrentamento da criminalidade digital. A investigação de crimes cibernéticos exige conhecimentos especializados em tecnologia da informação, análise de evidências digitais e rastreamento de atividades online, competências que nem sempre estão plenamente disponíveis nas instituições responsáveis pela persecução penal.

Além disso, a própria regulação do ambiente digital envolve desafios relacionados à proteção de dados pessoais e à atuação de empresas que operam serviços baseados na coleta e tratamento de informações dos usuários. Como observa Wendt (2023, p. 117), a coleta de dados pessoais por provedores de conexão e aplicações na Internet constitui um segmento capaz de gerar danos em grande escala, razão pela qual diversos países têm buscado desenvolver legislações específicas para regulamentar o tratamento dessas informações.

Nesse sentido, a criação da Lei Geral de Proteção de Dados representou um avanço importante no cenário jurídico brasileiro, alinhando o país a tendências internacionais de proteção à privacidade e ao tratamento responsável de dados pessoais. Contudo, a efetividade dessa legislação depende da implementação de mecanismos adequados de fiscalização, da atuação das autoridades reguladoras e da conscientização das organizações quanto à importância da proteção de dados.

Por outro lado, é importante reconhecer que a regulação jurídica da Internet não pode ser compreendida como solução absoluta para todos os problemas decorrentes do ambiente digital. Conforme argumenta Wendt (2023, p. 117), nem a governança global nem a regulamentação local são capazes de eliminar completamente as diferenças culturais, institucionais e organizacionais existentes entre os diversos sistemas jurídicos. Assim, a dimensão prática da atuação de instituições como polícia, Ministério Público e Poder Judiciário assume papel fundamental na efetividade da aplicação das normas relacionadas ao ambiente digital.

Diante desse cenário, torna-se evidente que os avanços legislativos alcançados pelo Brasil nas últimas décadas representam apenas uma etapa inicial no processo de construção de um sistema jurídico adequado à sociedade digital. A

complexidade das relações estabelecidas na Internet exige constante atualização normativa, bem como a adaptação das instituições responsáveis pela aplicação do Direito.

Portanto, embora legislações como a Lei Carolina Dieckmann, o Marco Civil da Internet e a Lei Geral de Proteção de Dados tenham contribuído para fortalecer a proteção jurídica no ambiente digital, persistem desafios relevantes relacionados à cooperação internacional, à capacitação institucional, à evolução tecnológica e à necessidade de constante aperfeiçoamento do arcabouço normativo. Nesse sentido, o desenvolvimento de políticas públicas, investimentos em formação especializada e aprimoramento da legislação são medidas essenciais para que o Direito consiga acompanhar as transformações impostas pela sociedade digital e enfrentar de forma eficaz os desafios decorrentes da criminalidade cibernética.

CAPÍTULO 3 - DESAFIOS DA INVESTIGAÇÃO CRIMINAL NO BRASIL

A análise do marco jurídico brasileiro, desenvolvida no capítulo anterior, demonstrou que o ordenamento nacional avançou de forma consistente, ainda que tardia, na construção de instrumentos normativos voltados ao enfrentamento do cibercrime. A Lei Carolina Dieckmann inaugurou a tipificação específica das invasões digitais, já o Marco Civil da Internet disciplinou as relações no ambiente virtual e criou obrigações de guarda de registros que dão suporte à investigação criminal. A LGPD consolidou a proteção de dados como direito fundamental densificado normativamente. Esse arcabouço, embora incompleto, existe e opera.

O problema que se coloca neste capítulo é de outra ordem, diz respeito à existência de normas adequadas é como condição necessária, mas não suficiente, para a efetividade da persecução penal, o que evidencia que o modelo brasileiro de enfrentamento ao cibercrime padece menos de lacunas legislativas e mais de deficiências estruturais e operacionais. Entre o texto legal e a responsabilização concreta do agente criminoso existe um conjunto de obstáculos práticos, técnicos e institucionais que a norma, por si só, não é capaz de superar. Como aponta Wendt (2024), a atuação efetiva no campo do cibercrime exige muito mais do que legislação, exige estrutura, método, capacitação e cooperação. O presente capítulo examina precisamente esse conjunto de obstáculos, organizados em quatro eixos analíticos: a preservação da prova digital, os limites da cooperação internacional, os desafios impostos pelas técnicas de anonimização e perícia, e as limitações estruturais dos órgãos de persecução penal.

3.1 A VOLATILIDADE E PRESERVAÇÃO DA PROVA DIGITAL

3.1.1 Natureza jurídica e características técnicas da evidência digital

A prova digital pode ser compreendida como todo dado ou conjunto de dados gerado, transmitido, recebido ou armazenado em suporte eletrônico, óptico ou similar, dotado de relevância para a demonstração de fatos no processo penal. Essa definição, embora aparentemente simples, encobre uma complexidade técnica que

desafia as categorias tradicionais do Direito Probatório, categorias desenvolvidas para um universo de evidências físicas, documentais e testemunhais que obedecem a lógicas completamente distintas.

A primeira e mais determinante característica da evidência digital é sua volatilidade estrutural. Diferentemente de um documento impresso, que permanece fisicamente intacto enquanto não é fisicamente destruído, os dados digitais existem sobre suportes em permanente operação, memórias que se sobrescrevem, conexões que se encerram, *logs* que expiram, arquivos temporários que são apagados por rotinas automáticas do sistema. Como alertam Barreto, Kufa e Silva (2021), a simples inicialização de um dispositivo já pode modificar dados de registro que seriam essenciais à investigação. O investigador que chega ao local de um crime digital enfrenta, portanto, um ambiente probatório que se autodestrói na ausência de intervenção técnica imediata e correta.

A segunda característica é a reprodutibilidade perfeita associada à fragilidade de autenticidade. Um arquivo digital pode ser copiado com absoluta fidelidade, o que, em princípio, facilita a preservação, mas essa mesma característica torna impossível distinguir, sem metodologia forense adequada, uma cópia íntegra de uma cópia adulterada. Um log de acesso (registro de todas as solicitações de arquivos individuais que as pessoas ou aplicações solicitam de um sistema) pode ser modificado sem deixar rastros visíveis ao exame ordinário. É justamente por isso que o conceito de cadeia de custódia assume, na prova digital, exigências técnicas muito mais rigorosas do que as aplicáveis às evidências físicas convencionais.

A terceira característica é a dispersão e ubiquidade. Uma investigação típica de cibercrime pode demandar evidências armazenadas simultaneamente em dispositivos físicos apreendidos, em servidores nacionais, em plataformas operadas por empresas estrangeiras e em serviços de computação em nuvem cujos dados se distribuem fisicamente por data centers em países diferentes. Essa dispersão transforma a coleta de prova digital em operação multijurisdicional por natureza.

Para fins de análise forense, a doutrina especializada distingue ao menos três categorias de evidência digital com graus diferentes de volatilidade: os dados armazenados (*stored data*), como arquivos em disco rígido ou memória flash; os dados transmitidos (*transmitted data*), como pacotes em trânsito em redes; e os dados processados (*processed data*), presentes em memória volátil durante a execução de programas (CASEY, 2011). Cada categoria demanda técnicas distintas de coleta e

preservação. Nesse contexto, destaca-se também a relevância dos registros técnicos para identificação dos usuários no ambiente digital, uma vez que “o protocolo de internet é a identidade digital do usuário. Em regra, permite individualizar o responsável por determinada conduta ao utilizar um serviço” (BARRETO; KUFA; SILVA, 2021, p. 144). A não compreensão dessas diferenças pelos operadores do direito, e isso inclui delegados, promotores e juízes, frequentemente resulta em mandados de busca e apreensão digitais mal formulados, que não especificam quais tipos de dados devem ser buscados nem impõem as condições técnicas mínimas para sua coleta adequada e subsequente preservação.

3.1.2 A cadeia de custódia da prova digital após a Lei nº 13.964/2019

A Lei nº 13.964/2019, o Pacote Anticrime, introduziu no Código de Processo Penal, por meio dos artigos 158-A a 158-F, uma disciplina expressa da cadeia de custódia. O artigo 158-A define cadeia de custódia como "o conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte." As etapas estabelecidas pelo artigo 158-B: reconhecimento, isolamento, fixação, coleta, acondicionamento, transporte, recebimento, processamento, armazenamento e descarte, foram concebidas com base no universo da criminalística tradicional, mas sua aplicação à prova digital tem sido progressivamente reconhecida como necessária pela doutrina e pelos tribunais.

O problema é que essa transposição não é automática. A preservação de um dispositivo eletrônico em uma busca e apreensão exige procedimentos que a legislação não descreve. Nesse sentido merece destaque o isolamento do aparelho de redes sem fio para evitar alteração remota de dados; a utilização de bloqueadores de escrita (*write blockers*) durante a cópia forense; a geração de *hash* criptográfico (código hash) do conteúdo original para atestar a integridade da cópia; o acondicionamento em embalagem antiestática (gaiola de Faraday). Nenhum desses passos está previsto no CPP. A regulamentação desses procedimentos é remetida a normas técnicas e manuais operacionais dos próprios órgãos de investigação, gerando heterogeneidade de práticas e fragilidade na demonstração posterior de confiabilidade da prova em juízo.

A Convenção de Budapeste, internalizada pelo Decreto nº 11.491/2023, avança nessa direção ao estabelecer, em seus artigos 16 e 17, obrigações de

preservação expedita de dados armazenados e preservação e divulgação parcial de dados de tráfego. Esses dispositivos criam para os Estados Partes o dever de dispor de mecanismos que permitam a preservação imediata de dados digitais identificados como potencialmente relevantes para investigações, inclusive antes de iniciado o procedimento formal de cooperação policial ou judiciária. A internalização desse instrumento pelo Brasil, ocorrida em 2023, é avanço significativo, mas sua efetividade prática depende da implementação de estruturas operacionais ainda em construção.

Do ponto de vista jurisprudencial, o Superior Tribunal de Justiça tem enfrentado a questão com frequência crescente. A orientação que emerge dos julgamentos mais recentes é no sentido de que a inobservância da cadeia de custódia não gera nulidade automática da prova, exigindo-se demonstração de efetivo prejuízo à defesa, aplicação do princípio pas de nullité sans grief. Essa posição é compreensível do ponto de vista da pragmática processual, mas tem sido alvo de crítica doutrinária fundada. Lopes Jr. (2022) sustenta que, no caso da prova técnica digital, o rompimento da cadeia de custódia não é um vício processual como os demais.Trata-se de uma impossibilidade epistêmica, uma vez que não há como atestar a integridade da evidência, se o julgador não sabe se está diante do dado original ou de uma versão alterada, e essa incerteza não pode ser superada pela simples ausência de prejuízo demonstrável, porque o prejuízo é justamente não saber se há prejuízo.

Essa crítica aponta um problema sério no nosso sistema de justiça criminal, ou seja, quando uma prova digital é produzida de forma descuidada, a lei não exige que o investigador demonstre que ela foi preservada corretamente, gerando a indesejada e ilegal inversão do ônus da prova.

O resultado é concreto é que os laudos de qualidade técnica duvidosa chegam ao julgamento sem que ninguém tenha verificado, de fato, se os dados não foram alterados ou corrompidos ao longo do caminho. Isso compromete não apenas a confiabilidade daquelas provas específicas, mas a credibilidade do processo penal como um todo nos crimes cibernéticos.

3.1.3 Desafios práticos na coleta e na requisição de dados a provedores

Os problemas da preservação da prova digital manifestam-se em três momentos críticos distintos: a coleta no local, a solicitação de registros a provedores e a análise forense posterior.

Na busca e apreensão, o problema central é a atuação dos policiais (militares ou civis) sem formação técnica especializada em forense digital. A INTERPOL, em seus protocolos para o primeiro contato com as evidências digitais, estabelece ações mínimas que incluem não acionar dispositivos desligados, não desligar dispositivos ligados sem avaliação técnica, isolar o ambiente de redes sem fio e registrar fotograficamente o estado dos equipamentos antes de qualquer manuseio. A ausência de treinamento básico nessa área entre os profissionais que chegam primeiro ao local de um crime é uma das causas mais frequentes de comprometimento irreversível de evidências digitais. Como observa Wendt (2024), a padronização e o treinamento de equipes são elementos essenciais para a atuação eficaz em contextos tecnológicos, e essa é precisamente a lacuna que mais onera o início das investigações.

Na requisição de dados a provedores, o regime do Marco Civil da Internet, conforme analisado no capítulo anterior, estabelece prazos de guarda e exige autorização judicial para a quebra de sigilo. O problema prático, contudo, não está apenas no regime jurídico, mas na velocidade e completude com que esses registros são efetivamente entregues após a ordem judicial. Provedores de menor porte frequentemente não dispõem de estrutura jurídica para processar requisições com rapidez, e entregas parciais ou incompletas comprometem o fluxo investigativo. A situação se agrava quando os dados já não existem mais nesse sentido seis meses de guarda de registros de aplicação podem ser insuficientes para investigações que apenas se iniciam após denúncias tardias das vítimas. A UNODC, em seus materiais técnicos sobre evidência eletrônica (2019), recomenda que os Estados considerem a extensão dos prazos de retenção como medida de adequação normativa, perspectiva ainda não acolhida legislativamente no Brasil.

Na análise forense, mesmo que a coleta tenha sido tecnicamente correta, a produção da prova exige equipamentos especializados, softwares licenciados, como sistemas de extração de dados de dispositivos móveis e plataformas de análise forense, e peritos habilitados para traduzir os resultados técnicos em linguagem jurídica compreensível ao processo. Mas importa registrar aqui um aspecto processual frequentemente negligenciado: como demonstrar ao juiz que o arquivo apresentado como prova é idêntico ao dado original coletado? A resposta técnica decorre da comparação de funções hash criptográficas, que é simples para um perito em computação, mas completamente opaca para a maioria dos operadores do direito. Essa assimetria cognitiva entre peritos e julgadores representa um desafio à

efetividade do processo penal, gerando tanto o risco de rejeição injustificada de provas tecnicamente sólidas quanto o de aceitação acrítica de evidências comprometidas.

3.1.4 Lacunas institucionais e perspectivas de padronização

No plano institucional, a ausência de um protocolo nacional unificado para a preservação da prova digital é a lacuna mais significativa. Enquanto delegacias especializadas em alguns estados adotam padrões técnicos próximos às melhores práticas internacionais, muitas unidades policiais carecem de conhecimentos elementares sobre como proceder diante de um dispositivo eletrônico encontrado em um local de crime. Essa heterogeneidade compromete a isonomia investigativa e contribui para que crimes praticados em estados com menor estrutura forense tenham probabilidade significativamente menor de resultar em responsabilização penal efetiva.

O Ministério Público Federal já demonstrava preocupação com a padronização da atuação em matéria de crimes cibernéticos por meio do Roteiro de Atuação sobre Crimes Cibernéticos, publicado em 2013 pela então Vigésima Nona Câmara de Coordenação e Revisão (MPF, 2013). Embora elaborado em momento anterior à introdução da disciplina legal da cadeia de custódia pelo Pacote Anticrime e à adesão brasileira à Convenção de Budapeste, o documento evidencia um esforço institucional inicial de sistematização de procedimentos investigativos em ambiente digital. Posteriormente, o desenvolvimento legislativo e normativo passou a exigir a constante atualização dessas diretrizes para adequá-las às novas exigências jurídicas e técnicas.

No tocante à sanção originalmente prevista, a redação inicial do art. 154-A do Código Penal, introduzida pela Lei nº 12.737/2012, estabelecia pena de detenção de três meses a um ano, além de multa. A doutrina criticou a desproporcionalidade da reprimenda, considerada demasiadamente branda diante da gravidade potencial das condutas (BARRETO; KUFA; SILVA, 2021, p. 134). A baixa pena abstratamente cominada, além de dificultar medidas cautelares mais severas, esvaziava, na prática, o caráter dissuasório da norma, o que levou à sua posterior alteração pela Lei nº 14.155/2021, evidenciando o reconhecimento legislativo da insuficiência da resposta penal originalmente prevista.

3.2 COOPERAÇÃO INTERNACIONAL E QUESTÕES DE JURISDIÇÃO

3.2.1 Os limites da territorialidade clássica

O Direito Penal brasileiro foi construído sobre o princípio da territorialidade estabelecido no artigo 5º do Código Penal, ou seja, a lei penal se aplica a crimes cometidos no território nacional. Esse princípio pressupõe que o crime tem local definido e que as evidências podem ser coletadas dentro de um espaço físico delimitado. O cibercrime rompe todas essas pressuposições de forma simultânea.

Como já evidencia o Capítulo 1 desta pesquisa, a prática de um crime digital pode envolver múltiplos países em um único episódio criminoso, o agente está em um Estado, utiliza servidores situados em um segundo, as vítimas estão em um terceiro, e os dados relevantes estão armazenados em serviços de nuvem cujos data centers se distribuem por uma quarta e quinta jurisdições. Nenhum desses Estados, individualmente, detém o quadro completo, e as regras de extraterritorialidade previstas no artigo 7º do Código Penal, embora existentes, pressupõem que a investigação já avançou a ponto de identificar o autor e localizá-lo, o que frequentemente não é possível sem cooperação internacional prévia.

No plano interno, a questão da competência territorial entre os estados brasileiros também apresenta complexidade própria. O artigo 70 do Código de Processo Penal fixa a competência pelo local onde a infração se consumou. No ambiente digital, a definição desse local é frequentemente ambígua, como por exemplo onde seria o local de consumação de um crime de estelionato praticado pela internet: no local do servidor, no local do agente, no local onde a vítima acessou o sistema ou no local onde teve o prejuízo patrimonial? O STJ tem construído soluções casuísticas para essa questão, em linhas gerais fixando a competência no local do resultado lesivo para a vítima, mas a ausência de regra expressa no CPP para crimes digitais gera instabilidade jurisdicional que prejudica tanto a celeridade investigativa quanto a segurança jurídica do processo.

Como observam Barreto, Kufa e Silva (2021, p. 70), "muito da dificuldade encontrada no combate ao cibercrime advém da própria natureza do meio onde ocorre uma parte dos (ou todos os) atos executórios do delito: o ciberespaço", definido como espaço indefinido de transações e comunicações que não conhece limitações físicas. Essa natureza do ciberespaço é, simultaneamente, a razão pela qual o cibercrime se

expande globalmente com tanta facilidade e a razão pela qual a resposta estatal baseada em territorialidade encontra limites estruturais tão pronunciados.

3.2.2 A Convenção de Budapeste e o Decreto nº 11.491/2023

A Convenção sobre o Cibercrime do Conselho da Europa, celebrada em Budapeste em 23 de novembro de 2001, é o principal instrumento multilateral de direito internacional dedicado ao cibercrime. Seus três eixos fundamentais são: a harmonização normativa, mediante obrigações de tipificação de condutas; a modernização processual, com previsão de medidas específicas como preservação expedita de dados, busca e apreensão de dados informáticos e interceptação em tempo real; e a cooperação internacional acelerada, por meio de mecanismos que permitem solicitações urgentes entre países signatários, incluindo a rede de pontos de contato disponíveis vinte e quatro horas por dia, sete dias por semana (rede 24/7), prevista no artigo 35.

O Brasil, após longo processo de tramitação, ratificou a Convenção pelo Decreto Legislativo nº 37/2021 e a promulgou internamente por meio do Decreto nº 11.491, de 12 de abril de 2023. Do ponto de vista normativo, essa internalização vincula formalmente o Estado brasileiro aos mecanismos de cooperação acelerada e às obrigações de preservação expedita de dados, o que, como visto na seção 3.1, tem repercussão direta sobre a volatilidade da prova digital. Do ponto de vista operacional, a adesão à rede 24/7 significa que o Brasil passa a dispor de um ponto de contato permanente para solicitações urgentes de cooperação entre autoridades competentes, papel que recai principalmente sobre a Diretoria de Crimes Cibernéticos da Polícia Federal (DCIBER) e sobre a estrutura de cooperação internacional do Ministério Público Federal.

Esse avanço é concreto e relevante. Mas é necessário registrar as limitações do instrumento. A Convenção de Budapeste foi negociada no final dos anos 1990, antes da computação em nuvem massificada, das redes de anonimização de segunda e terceira geração e da disseminação das criptomoedas como meio de negociação moderno. O Segundo Protocolo Adicional à Convenção, aberto à assinatura desde 2022, busca enfrentar essas lacunas ao prever mecanismos de cooperação direta com provedores de serviços de outros Estados e de acesso transfronteiriço a dados em nuvem, mas está em fase de adesão pelos países signatários, e o Brasil ainda

precisará considerar sua ratificação como próxima etapa de alinhamento aos padrões internacionais.

Conforme já destacavam Barreto, Kufa e Silva (2021, p. 121), "obstaculizar a cooperação internacional é dar azo à criação de paraísos de cibercriminosos, a exemplo do que acontece com os paraísos fiscais". A internalização da Convenção de Budapeste é o passo mais significativo dado pelo Brasil nessa direção, mas sua efetividade depende de estruturação operacional que ainda está em construção.

3.2.3 MLATs, INTERPOL e os mecanismos concretos de cooperação

Para além da Convenção de Budapeste, a cooperação internacional penal se apoia no Brasil em uma rede de acordos bilaterais de auxílio jurídico mútuo, os Mutual Legal Assistance Treaties (MLATs), celebrados com países como Estados Unidos, Portugal, Itália, Espanha e outros, além da cooperação no âmbito da INTERPOL e da UNODC.

O MLAT com os Estados Unidos tem importância particular para a investigação de crimes cibernéticos, dado que as principais plataformas de tecnologia, como Google, Meta, Apple, Microsoft, Amazon, estão sediadas em território americano. Solicitações de dados de usuários nessas plataformas seguem, em regra, o procedimento do MLAT, que consiste transmissão do pedido ao Departamento de Justiça americano, análise de admissibilidade e apresentação dos dados em juízo nos Estados Unidos antes de sua transmissão ao Brasil. Esse processo, revestido das garantias processuais necessárias, pode levar meses, tempo incompatível com a volatilidade dos dados que se pretende obter, o que revela a inadequação dos mecanismos tradicionais de cooperação internacional frente à dinâmica acelerada do cibercrime.

Essa morosidade não é exclusiva do Brasil. É um problema estrutural dos mecanismos tradicionais de MLAT, reconhecido internacionalmente. Alguns países têm negociado acordos de acesso direto, como o UK-US CLOUD Act Agreement firmado entre Estados Unidos e Reino Unido em 2022, que permite às autoridades de um país solicitar dados diretamente às empresas de tecnologia do outro, sem passar pelo procedimento formal de MLAT. O Brasil não dispõe de instrumento equivalente com nenhum país, mantendo sua investigação de cibercrime dependente do mecanismo convencional com todas as suas limitações de tempo e procedimento.

No plano da INTERPOL, a organização disponibiliza às suas forças- membro ferramentas relevantes para a cooperação em cibercrime, incluindo o I- 24/7 (sistema global de comunicações policiais seguro), as Notícias Vermelhas a red notice (difusão vermelha) para localização e detenção de foragidos, e o grupo de trabalho especializado em cibercrime. A Polícia Federal brasileira tem engajamento ativo nesse sistema, embora os detalhes operacionais desse engajamento devam ser verificados junto às publicações institucionais da própria organização.

Como apontam Hufnagel, Harfield e Bronitt, o funcionamento eficaz da cooperação policial e judicial "exige muito mais do que celebração de acordos estabelecendo procedimentos": exige conhecimento profundo das estruturas dos sistemas penais estrangeiros envolvidos, domínio de como as coisas funcionam na prática e investimento contínuo na formação dos profissionais chamados a cooperar (HUFNAGEL; HARFIELD; BRONITT, 2012, p. 12). Essa observação, trazida pelos autores do ponto de vista da cooperação transnacional em geral, é especialmente aguda quando aplicada ao cibercrime, em que a velocidade tecnológica dos criminosos tende a superar a velocidade burocrática dos mecanismos de cooperação.

3.2.4 O problema das plataformas estrangeiras e os limites da jurisdição nacional

Um dos pontos de maior tensão prática na investigação de crimes cibernéticos reside na relação entre as autoridades brasileiras e as grandes empresas de tecnologia sediadas no exterior. O artigo 11 do Marco Civil da Internet estabelece que as empresas que oferecem serviços ao público brasileiro estão sujeitas à legislação e à jurisdição nacionais, independentemente da localização de seus servidores. Essa disposição tem sido invocada por autoridades judiciais para fundamentar ordens de entrega de dados dirigidas diretamente a plataformas estrangeiras, sem necessidade de recurso ao MLAT.

A efetividade dessas ordens, contudo, é variável. Para dados de cadastro, identificação do usuário, endereço de e-mail, número de telefone, empresas como Google e Meta geralmente cumprem ordens judiciais brasileiras por meio de portais de solicitação legal. Para dados de conteúdo, mensagens, e- mails, arquivos, a maioria das empresas exige o procedimento de MLAT ou invoca limitações decorrentes da legislação do país onde estão sediadas, como o Electronic Communications Privacy Act americano. Há ainda o caso específico dos aplicativos

de mensagens com criptografia de ponta a ponta, como no caso do WhatsApp, nos quais a própria empresa declara não ter acesso ao conteúdo das comunicações, questão desenvolvida na seção seguinte.

Do ponto de vista processual, o recurso a ordens judiciais dirigidas diretamente a provedores estrangeiros, sem a mediação do MLAT, suscita questões relevantes sobre a validade e admissibilidade dos dados assim obtidos. A ausência de reciprocidade formal e de supervisão judicial no país de origem pode comprometer a cadeia de custódia internacional da prova e abrir espaço para questionamentos defensivos sobre a licitude das evidências. Essa é uma área em que a doutrina processual penal brasileira ainda tem muito a construir.

3.3 TÉCNICAS DE ANONIMIZAÇÃO, CRIPTOGRAFIA E PERÍCIA DIGITAL

3.3.1 O ecossistema de anonimização: implicações investigativas e probatórias

A utilização de Redes Privadas Virtuais (VPNs) mascara o endereço IP real do usuário, interpondo entre o dispositivo e a internet um servidor intermediário que assume a identificação de origem. Do ponto de vista investigativo, isso significa que o endereço IP registrado nos logs do provedor atacado ou da plataforma onde a conduta ilícita foi praticada não pertence ao agente criminoso, mas ao servidor VPN, frequentemente sediado em país com legislação de privacidade restritiva, que não colabora com pedidos de dados de autoridades estrangeiras. A identificação do usuário real por trás de uma VPN depende do sucesso de um pedido de cooperação com o provedor do serviço ou do emprego de técnicas de correlação de tráfego, procedimentos demorados, tecnicamente complexos e frequentemente infrutíferos.

A rede Tor (normalmente utilizada por usuários da Deep Web) representa nível superior de anonimização. Como descrevem Barreto e Santos (2019), ao analisar o submundo da internet, o Tor roteia o tráfego do usuário por uma cadeia de ao menos três nós operados voluntariamente por usuários ao redor do mundo, criptografando o tráfego em camadas sucessivas de forma que nenhum nó individual conhece simultaneamente a origem, o destino e o conteúdo da comunicação. Essa arquitetura é justamente a que sustenta o acesso às chamadas camadas mais

profundas da internet, os ambientes onde, como registram os autores, "criminosos encontraram terreno fértil para o cometimento de ilícitos" (BARRETO; SANTOS, 2019, p. 84). Do ponto de vista forense, a identificação de um usuário Tor por análise de tráfego é extremamente difícil em condições normais, embora não absolutamente impossível mediante técnicas avançadas de análise de correlação temporal.

As criptomoedas adicionam dimensão financeira à anonimização. Enquanto o Bitcoin é tecnicamente rastreável por meio da análise da blockchain pública, e existem empresas especializadas nessa análise, as chamadas *privacy coins* como Monero foram especificamente projetadas para tornar a rastreabilidade das transações computacionalmente inviável. O uso de criptomoedas como instrumento de pagamento em mercados ilícitos da dark web e como mecanismo de lavagem de ativos obtidos em crimes cibernéticos representa desafio específico que a investigação financeira tradicional não está equipada para enfrentar.

Do ponto de vista jurídico, essas tecnologias não afastam a antijuridicidade da conduta. O crime se consumou independentemente de como o agente tentou ocultar sua identidade. Contudo, dificultam sobremaneira a prova da autoria, elemento subjetivo indispensável à responsabilização penal. A investigação que consegue identificar o endereço IP de origem de um ataque enfrenta, na sequência, a tarefa de demonstrar que aquele IP correspondia ao dispositivo usado pelo acusado, e não a uma VPN, a um dispositivo de terceiro comprometido ou a um acesso por rede pública. Essa cadeia de demonstrações exige expertise técnica, tempo e recursos que muitas vezes não estão disponíveis.

Ainda assim, a doutrina aponta que, apesar das dificuldades, a rastreabilidade no ambiente digital não é absolutamente inviável. A adequada preservação e análise dos vestígios eletrônicos pode permitir a reconstrução dos fatos e contribuir para a identificação dos responsáveis pela prática delitiva, evidenciando a importância da atuação pericial especializada.

3.3.2 Criptografia de ponta a ponta: o dilema estrutural da investigação criminal

A criptografia de ponta a ponta (*end-to-end encryption*, E2EE), implementada por aplicativos amplamente utilizados no Brasil como o WhatsApp e outros, garante que apenas os participantes de uma comunicação podem ler seu conteúdo. Nem o provedor do serviço, nem terceiros, nem as autoridades, mesmo munidas de ordem judicial, têm acesso ao conteúdo das mensagens criptografadas. Essa característica

coloca o investigador diante de uma impossibilidade técnica que a norma processual não foi desenhada para enfrentar.

O tema chegou ao Supremo Tribunal Federal por via do Recurso Extraordinário nº 1.037.396/SP, no qual se discutiram, entre outras questões, os limites da responsabilização de provedores de aplicação que alegam impossibilidade técnica de cumprir ordens de entrega de dados criptografados. O STF firmou entendimento no sentido de que a suspensão do aplicativo como medida sancionatória é desproporcional quando a empresa demonstra impossibilidade técnica de cumprimento, reconhecendo implicitamente, que a arquitetura de criptografia ponta a ponta cria uma limitação que o sistema processual brasileiro ainda não tem resposta normativa adequada para equacionar. O conteúdo preciso do acórdão deve ser verificado diretamente na publicação oficial do STF, pois a discussão envolveu múltiplas teses e diferentes composições ao longo do julgamento.

O debate sobre a criação de backdoors, vulnerabilidades técnicas intencionalmente introduzidas nos sistemas de criptografia para uso exclusivo das autoridades, é intenso no plano internacional, mas a posição majoritária dos especialistas em segurança da informação é firme, no sentido de que qualquer vulnerabilidade introduzida em um sistema criptográfico não pode ser tecnicamente restrita ao uso governamental. Uma vez existente, ela pode ser explorada por qualquer agente que a descubra, comprometendo a segurança de todos os usuários. O custo coletivo de enfraquecer a criptografia supera, na avaliação desses especialistas, o benefício investigativo que se obteria em casos individuais.

Na prática da persecução penal brasileira, a impossibilidade de acesso ao conteúdo de comunicações E2EE tem deslocado o foco investigativo para elementos periféricos: metadados de conexão (quem falou com quem, quando e por quanto tempo, sem o conteúdo), dados de localização, informações de cadastro, análise de dispositivos físicos apreendidos e técnicas de inteligência de fontes abertas (OSINT). Essas alternativas, embora não substituam o conteúdo das comunicações, têm se revelado, em muitas investigações, suficientes para a construção de prova indireta robusta, especialmente quando combinadas entre si. A sofisticação dessas técnicas alternativas é, paradoxalmente, um dos frutos da pressão exercida pela criptografia sobre os métodos investigativos.

3.3.3 Forense digital: metodologia, padrões técnicos e desafios de produção probatória

A perícia forense digital é o conjunto de procedimentos científicos e técnicos aplicados à identificação, preservação, coleta, análise e apresentação de evidências digitais em contexto judicial. Sua natureza é essencialmente técnico- jurídica: não basta que o perito identifique a evidência. É necessário que o processo de identificação tenha sido realizado de forma suficientemente documentada e metodologicamente rigorosa para que seu resultado possa ser apresentado, compreendido e, sobretudo, contestado em juízo.

As metodologias de forense digital são objeto de padronização internacional. A norma ISO/IEC 27037:2012 estabelece os princípios internacionalmente reconhecidos para identificação, coleta, aquisição e preservação de evidências digitais. O National Institute of Standards and Technology (NIST) americano, por meio de seu programa de teste de ferramentas forenses, certifica plataformas de análise quanto à confiabilidade e precisão de seus resultados. No Brasil, não existe até o momento um equivalente nacional plenamente estruturado para certificação de ferramentas e metodologias de forense digital, o que amplia a dependência de padrões estrangeiros e pode gerar questionamentos defensivos sobre a adequação das ferramentas utilizadas pelas polícias.

O processo forense segue, em linhas gerais, as seguintes fases: identificação e documentação dos dispositivos; preservação, com geração de hash e cópia forense bitstream que replica byte a byte o conteúdo do dispositivo original sem alterá-lo; análise do conteúdo da cópia forense, busca de arquivos relevantes, recuperação de dados apagados, análise de metadados e reconstituição de atividades do sistema; e, por fim, apresentação em laudo pericial redigido em linguagem acessível ao julgador, com descrição metodológica suficiente para que o resultado possa ser verificado e contestado.

Do ponto de vista processual, o laudo deve satisfazer os requisitos do artigo 159 do CPP, que exige a realização da perícia por perito oficial e a elaboração de laudo que descreva minuciosamente o objeto examinado, os exames realizados e as conclusões. Na prática, laudos de forense digital produzidos no Brasil variam enormemente em qualidade, clareza e completude. É frequente que laudos técnicos redigidos em linguagem altamente especializada não expliquem ao julgador os

fundamentos metodológicos que sustentam suas conclusões, o que compromete tanto a compreensão judicial quanto o exercício do contraditório.

O direito ao contraditório pericial, assegurado pelo artigo 159, §5º, do CPP, dispositivo que garante às partes o direito de formular quesitos ao perito e indicar assistentes técnicos, é pouco exercido em casos de forense digital por ausência de assistentes técnicos especializados disponíveis às defesas, especialmente às assistidas pela Defensoria Pública. Essa assimetria técnica entre acusação e defesa é dimensão processual que merece atenção específica das políticas de acesso à justiça. Assim, sem capacidade de contestar tecnicamente a prova pericial digital, a defesa não exerce de forma plena as garantias do devido processo legal.

3.3.4 A prova de autoria em ambiente digital: desafios jurisprudenciais

A demonstração da autoria em crimes cibernéticos apresenta especificidades que a dogmática processual penal tradicional não antecipou. A autoria em um crime físico convencional é provada por uma combinação de evidências diretas e indiretas. Em crimes cibernéticos, a prova é quase integralmente indireta e mediada por evidências técnicas, o que impõe ao julgador uma dependência de interpretação do laudo pericial que não tem paralelo em outras categorias de delito.

A questão do endereço IP como elemento de identificação do autor merece atenção específica. O IP de onde partiu uma comunicação ilícita é, via de regra, a primeira pista de autoria disponível, mas ele identifica o contrato de acesso à internet, não o usuário concreto. O titular do contrato pode ser uma pessoa jurídica, um familiar, um vizinho que utiliza a rede, ou simplesmente alguém cujo roteador foi comprometido e utilizado por terceiro sem seu conhecimento. O STJ tem reiteradamente reconhecido, em sua jurisprudência sobre crimes cibernéticos, que o endereço IP, isoladamente considerado, é insuficiente para fundamentar condenação ou prisão preventiva, sendo necessária a identificação do usuário concreto do dispositivo no momento do crime. Essa exigência é tecnicamente correta, mas opera como fator de dificuldade investigativa adicional, pois a prova da utilização concreta do dispositivo por uma pessoa determinada em momento específico pode demandar análise forense de registros de atividade do sistema, de logs de autenticação e de dados biométricos, todos elementos que requerem tempo, equipamento e expertise especializados.

A materialidade dos crimes cibernéticos, por sua vez, frequentemente depende integralmente da prova digital, capturas de tela, logs de acesso, arquivos

apreendidos. Na ausência de laudo pericial que comprove a autenticidade e integridade desses materiais, a defesa tem fundamento técnico e jurídico para questionar a validade probatória do conjunto. Tribunais brasileiros têm enfrentado essa questão com graus variados de rigor, e a jurisprudência ainda não convergiu para um padrão consolidado sobre os requisitos mínimos de autenticação da prova digital para fins de admissibilidade processual, lacuna que representa risco tanto para a acusação, que pode ver sua prova contestada, quanto para a defesa, que pode se deparar com juízes que aceitam evidências digitais sem o escrutínio técnico necessário.

3.4 LIMITAÇÕES ESTRUTURAIS E CAPACITAÇÃO DOS ORGÃOS DE PERSECUÇÃO PENAL

3.4.1 O quadro institucional: delegacias especializadas, laboratórios e Ministério Público

A resposta institucional brasileira ao cibercrime organiza-se em torno de algumas estruturas especializadas que coexistem com um vasto conjunto de unidades policiais e ministeriais sem especialização na área. No âmbito federal, a Polícia Federal mantém a Unidade de Repressão a Crimes Cibernéticos (DCIBER) e a Secretaria Nacional de Segurança Pública – SENASP/DIOPI, ligada ao Ministério da Justiça e Segurança Pública, conta com o CiberLab (Laboratório de Inteligência Cibernética) como estrutura de referência nacional, com atribuições de investigação de crimes de repercussão nacional e de suporte às polícias estaduais. No âmbito estadual, delegacias especializadas em crimes cibernéticos existem em estados como São Paulo, Rio de Janeiro, Minas Gerais, Paraná e Rio Grande do Sul, mas estão ausentes ou têm presença meramente formal em muitas unidades da federação, especialmente no interior dos estados e nas regiões Norte e Centro-Oeste.

Esse quadro de concentração geográfica da especialização investigativa tem consequências práticas diretas. Crimes cibernéticos praticados em localidades sem delegacia especializada são investigados, quando o são, por unidades policiais sem treinamento adequado e sem equipamentos específicos. O resultado é uma assimetria investigativa que não corresponde à distribuição geográfica do cibercrime, que, por definição, não respeita limites territoriais e atinge vítimas em todo o país de forma relativamente uniforme.

Diante desse cenário, impõe-se a necessidade de adaptação constante das estruturas institucionais à realidade tecnológica contemporânea. Como observa Peck (2012, p. 45), “o Direito deve refletir a realidade da sociedade”, o que implica reconhecer que a transformação digital exige não apenas atualização normativa, mas também reestruturação prática dos órgãos de persecução penal.

O Ministério Público conta com núcleos especializados em crimes cibernéticos no âmbito federal e em alguns estados, como São Paulo e Goiás, mas a especialização ministerial na área ainda é muito mais exceção do que regra. A ausência de membros com formação técnica em forense digital pode comprometer a supervisão da atividade investigativa, a elaboração de denúncias tecnicamente precisas e a atuação em processos que envolvam prova digital complexa. Nesse contexto, evidencia-se a necessidade de investimento contínuo em capacitação especializada e no fortalecimento institucional dos órgãos responsáveis pela persecução penal.

Em termos de laboratórios forenses, a demanda por perícias digitais cresceu exponencialmente nas últimas décadas sem que a capacidade instalada acompanhasse esse crescimento. O resultado é o acúmulo de laudos pendentes que compromete a celeridade das investigações, e, por consequência, a validade de medidas cautelares que dependem de fundamentação pericial ou a possibilidade de instauração de ação penal dentro de prazos razoáveis.

3.4.2 Recursos humanos, formação técnica e a lacuna do perfil híbrido

A investigação efetiva de crimes cibernéticos demanda um perfil profissional que combina, de forma integrada, competências jurídicas e técnicas. Juridicamente através do conhecimento de processo penal, direitos fundamentais, regime de prova, cooperação internacional. Tecnicamente por meio de redes de computadores, sistemas operacionais, forense digital, análise de malware, protocolos de criptografia. Esse perfil híbrido é raro no mercado de trabalho em geral, e sua formação sistemática no âmbito das carreiras de segurança pública apresenta desafios institucionais que ainda não foram adequadamente enfrentados.

Como aponta Wendt (2024), a investigação em contextos tecnológicos complexos envolve profissionais de *offensive security*, análise de dados e especialistas em extração de informações de dispositivos, perfis que as estruturas de formação policial tradicional não foram desenhadas para produzir. As academias de

polícia, em sua maioria, ainda não integraram a forense digital e a investigação de crimes cibernéticos como disciplinas obrigatórias de formação básica, tratando o tema como especialização a ser buscada individualmente pelos interessados, via cursos de extensão, certificações privadas ou formação em parcerias com organismos internacionais. Essa abordagem atomizada resulta em concentração de expertise em poucos profissionais, sem transferência sistemática de conhecimento para o restante do corpo funcional.

O problema se replica na magistratura e no Ministério Público. Juízes e promotores que lidam com crimes cibernéticos frequentemente relatam dificuldades em compreender laudos periciais produzidos em linguagem técnica especializada, tornando-se dependentes de explicações dos próprios peritos, situação que compromete tanto a autonomia decisória do julgador quanto o exercício pleno do contraditório. Programas de capacitação continuada em Escolas de Formação e Aperfeiçoamento de Magistrados e Escolas do Ministério Público têm avançado nessa direção, mas ainda de forma pontual.

3.4.3 Integração institucional: entraves e iniciativas

A efetividade da persecução penal de crimes cibernéticos não depende apenas da qualidade individual de cada órgão, mas da capacidade de esses órgãos atuarem de forma integrada. A investigação de cibercrime envolve múltiplos atores: polícias federais e estaduais, Ministério Público, Receita Federal, Banco Central, COAF, cada um com suas atribuições próprias, sistemas de informação frequentemente incompatíveis e culturas institucionais distintas. Investigações que revelam conexões entre crimes cibernéticos e organizações criminosas com ramificações em diferentes estados frequentemente se fragmentam em inquéritos paralelos, sem aproveitamento recíproco das evidências já produzidas.

Em sentido positivo, a Estratégia Nacional de Segurança Cibernética (E-Ciber), estabelecida pelo Decreto nº 10.222/2020, prevê mecanismos de coordenação entre o Gabinete de Segurança Institucional da Presidência da República e os órgãos de segurança pública com atribuições na investigação criminal. O NIC.br e o CERT.br desempenham papel importante na coleta de estatísticas sobre incidentes cibernéticos e na orientação técnica a usuários e organizações, embora sua articulação com os órgãos de investigação criminal permaneça informal e pouco estruturada.

A lacuna mais significativa nesse plano é a ausência de um comando coordenado de resposta a incidentes cibernéticos graves que articule, de forma imediata e eficiente, a inteligência de segurança cibernética com a persecução penal. Quando um ataque de ransomware paralisa uma instituição pública, como ocorreu no episódio do Tribunal de Justiça do Rio Grande do Sul em 2024, referido no Capítulo 1 desta pesquisa, as respostas de contenção técnica e de investigação criminal ocorrem em trilhas paralelas que frequentemente não se alimentam mutuamente, comprometendo tanto a recuperação dos sistemas quanto a responsabilização dos autores.

3.4.4 Políticas públicas e perspectivas de fortalecimento

O diagnóstico das limitações estruturais não pode prescindir do reconhecimento das iniciativas em curso. A internalização da Convenção de Budapeste pelo Decreto nº 11.491/2023 cria compromissos formais que demandam ajustes operacionais concretos, funcionando como vetor de pressão para que o Estado brasileiro avance na estruturação de suas capacidades investigativas de forma juridicamente vinculada. A participação na rede 24/7 da Convenção, o engajamento com os programas de capacitação do Conselho da Europa e os esforços de harmonização normativa criados pela ratificação são passos concretos que não devem ser subestimados.

No plano tecnológico, a crescente incorporação de técnicas de inteligência de fontes abertas (OSINT) à prática investigativa representa caminho promissor. O OSINT, que compreende a coleta, análise e correlação de informações disponíveis publicamente em redes sociais, fóruns, registros públicos e outras fontes abertas, não enfrenta os obstáculos legais da interceptação de comunicações privadas e pode fornecer evidências relevantes sobre identidade e comportamento de agentes criminosos no ambiente digital. Como apontam Barreto, Kufa e Silva (2021), as fontes abertas constituem campo fértil para a investigação, e o desenvolvimento de capacidades específicas nessa área avança entre as forças de segurança, ainda que de forma não sistemática.

O que o quadro geral revela, ao final desta análise, é que o principal déficit da resposta brasileira ao cibercrime não é normativo, o arcabouço legal, embora imperfeito, existe, mas estrutural, técnico e de governança, o que demonstra a insuficiência de respostas baseadas exclusivamente em produção legislativa e impõe

a necessidade de reconfiguração institucional da persecução penal no ambiente digital. As normas que autorizam a coleta de prova digital existem, mas faltam peritos para produzi-la adequadamente. Os mecanismos de cooperação internacional estão sendo construídos, mas operam com lentidão incompatível com a volatilidade das evidências. Os órgãos especializados existem, mas sua distribuição geográfica é insuficiente e sua integração, precária. Esse diagnóstico aponta para a necessidade de políticas públicas deliberadas e sustentadas, e não apenas de reformas legislativas pontuais, dimensão que o capítulo seguinte se encarregará de examinar.

CONCLUSÃO

O presente trabalho permitiu demonstrar que os crimes cibernéticos constituem um dos principais desafios contemporâneos para sistema de justiça criminal, exigindo a revisão de categorias tradicionais do Direito Penal e Processual Penal diante das transformações impostas pela sociedade da informação. Verificou-se que a evolução histórica da criminalidade digital acompanha diretamente o avanço tecnológico, ampliando a complexidade das condutas ilícitas e exigindo respostas cada vez mais sofisticadas por parte do Estado.

No âmbito normativo, constatou-se que o ordenamento jurídico brasileiro avançou de forma significativa na construção de instrumentos voltados ao enfrentamento do cibercrime, especialmente com a tipificação de condutas específicas, a regulamentação do ambiente digital e o fortalecimento da proteção de dados pessoais. Todavia, evidenciou-se que tais avanços não são suficientes, por si sós, para assegurar a efetividade da persecução penal, na medida em que a mera existência de normas não elimina os obstáculos práticos enfrentados na investigação criminal.

A análise dos desafios investigativos revelou que a facilidade de alteração ou exclusão de um vestígio digital, a complexidade da cadeia de custódia, as limitações dos mecanismos de cooperação internacional, o uso de técnicas de anonimização e criptografia, bem como a insuficiência estrutural dos órgãos de persecução penal, constituem fatores determinantes para a dificuldade de responsabilização dos agentes envolvidos em crimes cibernéticos. Demonstrou-se, ainda, que tais elementos não atuam de forma isolada, mas se reforçam mutuamente, comprometendo a eficiência investigativa e a confiabilidade da prova produzida em juízo.

Nesse contexto, confirmou-se a hipótese de que os principais déficits no enfrentamento ao cibercrime não são meramente legislativos, mas predominantemente estruturais e institucionais. A fragmentação das atribuições, a baixa integração entre os órgãos de persecução penal e a carência de capacitação técnica evidenciam que o problema ultrapassa o plano normativo, exigindo uma abordagem mais ampla, baseada em governança integrada e fortalecimento das capacidades operacionais do Estado.

Verificou-se, ainda, que a efetividade das investigações em ambiente digital depende diretamente da adoção de protocolos técnicos padronizados, do

investimento em formação especializada, do aprimoramento dos mecanismos de cooperação internacional e da construção de políticas públicas coordenadas. A ausência desses elementos compromete não apenas a eficiência da persecução penal, mas também a legitimidade do próprio sistema de justiça criminal diante de um cenário de crescente complexidade tecnológica.

Dessa forma, conclui-se que o enfrentamento da criminalidade cibernética no Brasil exige a superação de modelos tradicionais de investigação, a consolidação de uma governança institucional integrada e o desenvolvimento de estratégias estruturadas e contínuas, capazes de acompanhar a dinâmica evolutiva do ambiente digital. Somente por meio da articulação e a complementaridade entre a norma vigente, a qualificação técnica dos quadros e a coordenação institucional será possível promover uma resposta estatal efetiva, compatível com os desafios impostos pela cibercriminalidade e com as necessárias garantias fundamentais do Estado Democrático de Direito.

REFERÊNCIAS

BARRETO, Alessandro Gonçalves; SANTOS, Hericson dos. *Deep web: investigação no submundo da internet*. São Paulo: Brasport, 2019.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. Artigos 5º e 7º. Rio de Janeiro, 1940.

BRASIL. Decreto-Lei nº 3.685, de 3 de outubro de 1941. Código de Processo Penal. Artigos 70, 158-A a 158-F e 159. Rio de Janeiro, 1941.

BRASIL. Decreto Legislativo nº 37, de 2021. Aprova o texto da Convenção sobre o Cibercrime. Diário Oficial da União, Brasília, 2021.

BRASIL. Decreto nº 10.222, de 5 de fevereiro de 2020. Aprova a Estratégia Nacional de Segurança Cibernética (E-Ciber). Diário Oficial da União, Brasília, 6 fev. 2020.

BRASIL. Decreto nº 11.491, de 12 de abril de 2023. Promulga a Convenção sobre o Cibercrime. Diário Oficial da União, Brasília, 13 abr. 2023.

BRASIL. Lei nº 13.964, de 24 de dezembro de 2019. Aperfeiçoa a legislação penal e processual penal. Diário Oficial da União, Brasília, 26 dez. 2019.

BRASIL. Supremo Tribunal Federal. Recurso Extraordinário nº 1.037.396/SP.

BRASIL. Superior Tribunal de Justiça. Jurisprudência sobre competência em crimes cibernéticos e sobre cadeia de custódia da prova digital.

BRITZ, Marjie T. *Computer forensics and cybercrime: an introduction*. New Jersey: Prentice Hall, 2009.

CASEY, Eoghan. *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*. 3. ed. Waltham: Academic Press, 2011.

CERT.BR. Estatísticas de incidentes de segurança em redes no Brasil. São Paulo: NIC.br. Disponível em: https://cert.br/stats. Acesso em: 28 mar. 2026.

CLOUGH, Jonathan. *Principles of Cybercrime*. New York: Cambridge University Press, 2010.

CONSELHO DA EUROPA. Convenção sobre o Cibercrime (CETS nº 185). Budapeste, 23 nov. 2001. Disponível em: https://www.coe.int/en/web/conventions/full-list?module=treatydetailCtreatynum=185. Acesso em: 21 mar. 2026.

CONSELHO DA EUROPA. *Second Additional Protocol to the Budapest Convention on Cybercrime* (CETS nº 224). Estrasburgo, 2022. Disponível em: https://www.coe.int/en/web/cybercrime. Acesso em: 22 mar. 2026.

CONSELHO NACIONAL DE JUSTIÇA (CNJ). Estudos e iniciativas sobre cadeia de custódia da prova digital. Brasília: CNJ.

G1. TJ-RS diz que sistema de informática do tribunal foi alvo de ataque hacker e é "muito grave". 2021. Disponível em: https://g1.globo.com/rs/rio-grande-do-sul/noticia/2021/04/29/tj-rs-diz-que-sistema-de-informatica-do-tribunal-foi-alvo-de-ataque-hacker-e-muito-grave.ghtml. Acesso em: 14 fev. 2026.

GONÇALVES, Victor Hugo Pereira. *Marco civil da internet comentado*. São Paulo: Atlas, 2016.

HUFNAGEL, Saskia; HARFIELD, Clive; BRONITT, Simon. *Cross-border law enforcement: regional law enforcement cooperation – European, Australian and Asia-Pacific perspectives*. New York: Routledge, 2012.

INTERPOL. *Guidelines for First Responders: Handling of Digital Evidence*. Lyon: INTERPOL.

ISO/IEC 27002.

ISO/IEC 27037:2012. *Information technology: Security techniques. Guidelines for identification, collection, acquisition and preservation of digital evidence*. Geneva: ISO, 2012.

LOPES JR., Aury. *Direito Processual Penal*. 19. ed. São Paulo: Saraiva Jur, 2022.

MINISTÉRIO PÚBLICO FEDERAL (Brasil). *Roteiro de atuação sobre crimes cibernéticos*. Brasília: MPF, 2013.

NIST: NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. NIST SP 800-101 Rev. 1: *Guidelines on Mobile Device Forensics*. Gaithersburg: NIST, 2014. Disponível em: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf. Acesso em: 27 mar. 2026.

MACHADO, André. Especialistas explicam como computador de Carolina Dieckmann foi hackeado. O Globo, 2012. Disponível em: https://oglobo.globo.com/rio/especialistas-explicam-como-computador-de-carolina-dieckmann-foi-hackeado-4895771. Acesso em: 7 mar. 2026.

PECK, Patrícia. *Direito Digital*. 5. ed. revista, atualizada e ampliada. São Paulo: Saraiva, 2012.

SÊMOLA, Marcos. *Gestão da segurança da informação: uma visão executiva*. Rio de Janeiro: Elsevier, 2003.

UNODC: UNITED NATIONS OFFICE ON DRUGS AND CRIME. *Electronic Evidence: a Basic Guide for First Responders*. Vienna: UNODC, 2019. Disponível em: https://www.unodc.org/unodc/en/cybercrime/cybercrime-repository.html. Acesso em: 25 mar. 2026.

WENDT, Emerson. *Investigação Criminal Cibernética no Brasil*. São Paulo: Mizuno, 2024.