PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA DE DIREITO, NEGÓCIOS E COMUNICAÇÃO
NÚCLEO DE PRÁTICA JURÍDICA
COORDENAÇÃO ADJUNTA DE TRABALHO DE CONCLUSÁO DE CURSO

A EVOLUÇÃO DOS CRIMES CIBERNÉTICOS: DESAFIOS DA INVESTIGAÇÃO DIGITAL E A ADAPTAÇÃO DA LEGISLAÇÃO FRENTE AO AVANÇO TECNOLÓGICO

ORIENTANDA – MARIA LUIZA SAMPAIO

ORIENTADOR - PROF. DR. GERMANO CAMPOS SILVA

GOIÂNIA-GO
2025

MARIA LUIZA SAMPAIO

A EVOLUÇÃO DOS CRIMES CIBERNÉTICOS: DESAFIOS DA INVESTIGAÇÃO DIGITAL E A ADAPTAÇÃO DA LEGISLAÇÃO FRENTE AO AVANÇO TECNOLÓGICO

Monografia Jurídica apresentada à disciplina Trabalho de Curso I, da Escola de Direito , Negócios e Comunicação da Pontifícia Universidade Católica de Goiás(PUCGOIÁS).
Orientador: Prof. Dr. Germano Campos Silva

GOIÂNIA-GO
2025

MARIA LUIZA SAMPAIO

A EVOLUÇÃO DOS CRIMES CIBERNÉTICOS: DESAFIOS DA INVESTIGAÇÃO DIGITAL E A ADAPTAÇÃO DA LEGISLAÇÃO FRENTE AO AVANÇO TECNOLÓGICO

Data da Defesa: _____de_____ de_____

BANCA EXAMINADORA

_____

Orientador (a): Prof. Dr. Germano Campos Silva Nota

_____

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

Agradecimentos

Gostaria de iniciar agradecendo a Deus, pois somente Ele conhece todas as dificuldades e as facilidades encontradas até aqui. Se alcancei este momento, é porque Ele guiou cada passo do meu caminho e me concedeu forças para seguir.

Agradeço à minha mãe, Daiane, meu exemplo de força, por permanecer firme ao meu lado, sem medir esforços para que este sonho se tornasse realidade. Sua dedicação, apoio e fé em meu potencial foram essenciais em toda a caminhada, seu único defeito é não ser eterna. Você sempre se desdobrou para que nada me faltasse, oferecendo não apenas cuidado, mas também inspiração e incentivo para que eu me tornasse uma pessoa melhor a cada dia. Sua confiança inabalável em mim e sua capacidade de enfrentar desafios me motivam constantemente.

Meu sincero agradecimento ao meu amor, Luismar, por estar sempre presente, me apoiando, incentivando, ajudando e acreditando em mim, mesmo quando eu duvidava de mim mesma. Sua parceria, seu companheirismo, e suas palavras de encorajamento foram fundamentais para que eu mantivesse a determinação e alcançasse este objetivo.

Agradeço também à minha colega e amiga Lara, pelo companheirismo, pela ajuda e pela parceria ao longo da graduação. Sua presença tornou essa caminhada mais leve e especial.

Por fim, estendo minha gratidão à coordenação e a todo o corpo docente, em especial aos professores Germano e Cristina, pelos ensinamentos, paciência, dedicação e valiosas contribuições. As orientações, discussões e feedbacks recebidos foram fundamentais para o desenvolvimento deste trabalho e para o meu crescimento acadêmico e pessoal.

Não cheguei até aqui por minhas próprias forças, eu cheguei até aqui porque a boa mão do Senhor está sobre mim.

Neemias 2:18

RESUMO

A era digital transformou profundamente a sociedade contemporânea, alterando as formas de comunicação, trabalho e interação, ao mesmo tempo em que criou novos desafios para o sistema jurídico-penal. O crescimento do uso da internet e das tecnologias da informação impulsionou o surgimento dos crimes cibernéticos, caracterizados pelo uso de dispositivos eletrônicos como meio ou objeto de condutas delituosas. A investigação desses crimes enfrenta obstáculos específicos, como o anonimato e a transnacionalidade das ações. No Brasil, legislações como a Lei Carolina Dieckmann (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) representaram avanços na proteção digital. Entretanto, a rápida evolução tecnológica exige constante atualização normativa e cooperação internacional. A Inteligência Artificial (IA) surge como ferramenta essencial na segurança digital, auxiliando na detecção e prevenção de ataques, mas também pode ser utilizada de forma ilícita, intensificando os riscos cibernéticos. Assim, a regulamentação ética e transparente da IA torna-se urgente. O enfrentamento dos crimes digitais demanda integração entre direito, tecnologia e segurança, além de investimento em capacitação e inovação. O futuro da segurança digital dependerá da agilidade legislativa e da colaboração entre diferentes áreas do conhecimento, visando um ambiente virtual mais seguro e justo.

Palavras-chave: Crimes cibernéticos; Direito digital; Inteligência Artificial; Segurança da informação; Legislação brasileira.

ABSTRACT

The digital era has profoundly transformed contemporary society, reshaping communication, work, and social interactions while creating new challenges for the legal and penal systems. The expansion of internet use and information technologies has led to the rise of cybercrimes, characterized by the use of electronic devices as means or objects of criminal conduct. Investigating these crimes poses unique challenges, such as anonymity and cross-border activity. In Brazil, laws such as the Carolina Dieckmann Law (Law No. 12,737/2012), the Internet Civil Framework (Law No. 12,965/2014), and the General Data Protection Law (Law No. 13,709/2018) have advanced digital protection. However, rapid technological evolution demands continuous legal adaptation and international cooperation. Artificial Intelligence (AI) emerges as a vital tool for cybersecurity, enhancing threat detection and prevention, yet it can also be exploited for illicit purposes, amplifying cyber risks. Therefore, ethical and transparent regulation of AI is urgent. Combating cybercrime requires the integration of law, technology, and security, along with investment in innovation and professional training. The future of digital security depends on legislative agility and multidisciplinary collaboration to ensure a safer and fairer cyberspace.

Keywords: Cybercrime; Digital law; Artificial Intelligence; Information security; Brazilian legislation.

SUMÁRIO

INTRODUÇÃO **10**

1 EVOLUÇÃO DOS CRIMES CIBERNÉTICOS **12**

1.1 PRIMEIROS REGISTROS DE CRIMES DIGITAIS 13

1.2 IMPACTO DO AVANÇO TECNOLÓGICO NO SURGIMENTO DE NOVAS MODALIDADES CRIMINOSAS 14

2 DESAFIOS DA INVESTIGAÇÃO DIGITAL **17**

2.1 A INVESTIGAÇÃO DIGITAL 17

3 LEGISLAÇÃO APLICÁVEL **22**

3.1 ANÁLISE DO MARCO CIVIL DA INTERNET 22

3.2 ANÁLISE DA LEI CAROLINA DIECKMANN 24

3.3 DISCUSSÃO SOBRE A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) 26

4 ANÁLISE DA EFICÁCIA DAS MEDIDAS LEGAIS **29**

4.1 AVANÇOS OBTIDOS COM A LEGISLAÇÃO EXISTENTE 29

4.2 IDENTIFICAÇÃO DE LACUNAS E A NECESSIDADE DE ATUALIZAÇÕES CONSTANTES 30

5 PERSPECTIVAS FUTURAS **32**

5.1 A INFLUÊNCIA DA INTELIGÊNCIA ARTIFICIAL NA SEGURANÇA DIGITAL 32

5.2 TENDÊNCIAS LEGISLATIVAS PARA ENFRENTAR NOVOS DESAFIOS TECNOLÓGICOS 32

5.3 EXPERIÊNCIAS INTERNACIONAIS DE LEGISLAÇÕES MAIS RIGOROSAS 34

CONCLUSÃO 36

REFERÊNCIAS 38

INTRODUÇÃO

A era digital trouxe consigo transformações profundas na sociedade contemporânea, revolucionando não apenas as formas de comunicação, trabalho e relacionamento, mas também criando novos desafios para o sistema jurídico-penal. O crescimento exponencial do uso da internet e das tecnologias da informação proporcionou o surgimento de modalidades criminosas inéditas, conhecidas como crimes cibernéticos ou crimes digitais, que se caracterizam pela utilização de dispositivos eletrônicos e redes de computadores como meio ou objeto para a prática de condutas delituosas.

Diferente dos crimes físicos, que muitas vezes deixam rastros evidentes, a investigação digital enfrenta desafios únicos, como a dificuldade em identificar os responsáveis por trás das infrações. O anonimato na internet, o uso de redes criptografadas e a possibilidade de cometer crimes a partir de qualquer lugar do mundo tornam a apuração desses delitos ainda mais complexa. Conforme observa Almeida (2015, p. 45), "os crimes cibernéticos representam um novo paradigma para o direito penal, exigindo adaptações legislativas e investigativas que acompanhem a velocidade das inovações tecnológicas". Para compreender esse cenário, torna-se fundamental analisar o surgimento e o desenvolvimento dos crimes digitais, as mudanças trazidas pelo crescimento da internet e os impactos na segurança cibernética, bem como as principais leis e regulamentações criadas para proteger usuários e punir atividades criminosas no ambiente virtual.

A transformação digital mudou radicalmente a forma como vivemos, nos relacionamos e trabalhamos. Desde os primeiros relatos de crimes envolvendo informática, na década de 1960, nos Estados Unidos, a utilização de computadores para fins ilícitos – como sabotagens e espionagem – já despertava a atenção da sociedade e da comunidade científica. Com o passar dos anos, principalmente a partir dos anos 1980, os delitos cibernéticos evoluíram, passando a abranger áreas como a manipulação de dados bancários, a pirataria de softwares, abusos nas telecomunicações e até a pornografia infantil.

Na década de 1990, a popularização dos computadores pessoais e, posteriormente, dos celulares, aliada ao crescimento das transações financeiras

online, fez com que os crimes cibernéticos se tornassem ainda mais comuns e impactantes. Recentemente, a pandemia de COVID-19 acelerou esse processo, aumentando significativamente os ataques virtuais, especialmente no setor do comércio eletrônico, e evidenciando a vulnerabilidade de indivíduos e instituições. Neste contexto, Cruz e Rodrigues (2018, p. 23) destacam que "a falsa sensação de impunidade no ambiente virtual contribui para o aumento dos crimes cibernéticos, tornando essencial o fortalecimento dos mecanismos de investigação e punição".

Essa pesquisa é extremamente relevante tanto do ponto de vista jurídico quanto social. No campo jurídico, é imprescindível que as leis acompanhem o ritmo acelerado das inovações tecnológicas para oferecer proteção eficaz contra fraudes, invasões de sistemas e o roubo de dados. Já do ponto de vista social, entender a legislação vigente e seus impactos é fundamental para que a população se conscientize sobre os riscos do ambiente digital e se proteja melhor contra os crimes cibernéticos.

O Brasil tem buscado adaptar seu ordenamento jurídico para enfrentar os desafios impostos pelos crimes digitais. A Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, representou um marco importante ao tipificar condutas como a invasão de dispositivos informáticos e a interrupção de serviços digitais. Posteriormente, o Marco Civil da Internet (Lei nº 12.965/2014) estabeleceu princípios, garantias, direitos e deveres para o uso da internet no Brasil, complementando o arcabouço legal de proteção no ambiente digital. Mais recentemente, a Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018) trouxe importantes avanços na proteção de dados pessoais, alinhando a legislação brasileira aos padrões internacionais.

Ao analisar criticamente a evolução legislativa, este estudo busca identificar avanços e lacunas na proteção dos usuários, além de apontar desafios práticos na investigação e punição de criminosos, especialmente em um cenário globalizado. Essa reflexão não só amplia nosso conhecimento sobre as mudanças no campo do Direito Digital, mas também estimula o debate sobre medidas preventivas e educativas que possam transformar a internet em um espaço mais seguro para todos.

CAPÍTULO 1
EVOLUÇÃO DOS CRIMES CIBERNÉTICOS

A história dos crimes cibernéticos está intrinsecamente ligada à evolução da tecnologia da informação. Desde os primeiros computadores até a internet das coisas, cada avanço tecnológico trouxe consigo novas oportunidades para a inovação, mas também novas vulnerabilidades exploradas por indivíduos e grupos com intenções maliciosas.

O Escritório das Nações Unidas sobre Drogas e Crime (UNODC) caracteriza os crimes cibernéticos como "uma forma de crime transnacional em expansão, cuja natureza complexa ocorre no ciberespaço, sem fronteiras" (UNODC, 2025). Esta definição enfatiza duas características fundamentais: a transnacionalidade e a ausência de limitações geográficas, aspectos que distinguem os crimes cibernéticos dos delitos tradicionais.

Já sobre uma perspectiva técnica a Kaspersky (2025), empresa especializada em segurança digital, define crime cibernético como uma atividade criminosa que tem como alvo ou faz uso de um computador, uma rede de computadores ou um dispositivo conectado em rede. Esta definição técnica destaca tanto os crimes que visam sistemas computacionais quanto aqueles que utilizam a tecnologia como instrumento.

A doutrina brasileira tradicionalmente classifica os crimes cibernéticos em duas categorias principais (Belezzi, Rosa, 2017):

1. Crimes Virtuais Próprios: São aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade das informações automatizadas. Estes crimes só podem ser praticados no ambiente digital e não possuem correspondente no mundo físico.
2. Crimes Virtuais Impróprios (ou Comuns): Correspondem aos crimes tradicionais que são praticados utilizando a internet como ferramenta. Nestes casos, o meio digital é apenas o instrumento para a prática de delitos já tipificados no ordenamento jurídico.

Esta seção traça a trajetória dos crimes digitais, desde seus primórdios até as complexas ameaças que enfrentamos hoje.

1.1 PRIMEIROS REGISTROS DE CRIMES DIGITAIS

Os primeiros registros de crimes digitais remontam a uma era em que os computadores eram máquinas gigantescas, acessíveis a um número restrito de pessoas. No entanto, mesmo nesse ambiente limitado, a curiosidade e a engenhosidade humana já demonstravam o potencial para o uso indevido da tecnologia. A década de 1940 marcou o nascimento da computação moderna, com a criação do primeiro computador digital em 1943. Nesse período, a ideia de crime cibernético ainda era ficção científica. No entanto, as bases teóricas para o que viria a ser uma das principais ferramentas dos criminosos digitais foram lançadas em 1949, quando o matemático John von Neumann especulou que programas de computador poderiam se autorreplicar, uma teoria que antecipou o conceito de vírus de computador (Chadd, 2020).

Na década de 1950, o foco da atividade precursora do hacking estava nos sistemas de telefonia. O "phone phreaking", que surgiu no final da década, consistia em explorar as frequências sonoras usadas pelas companhias telefônicas para fazer chamadas de longa distância gratuitamente. Os "phreaks", como eram conhecidos, formaram uma subcultura que compartilhava conhecimentos e técnicas, e entre seus membros estavam figuras que mais tarde se tornariam pioneiras da revolução dos computadores pessoais, como Steve Wozniak e Steve Jobs (Borges, 2024).

A década de 1960 testemunhou os primeiros casos documentados de crimes relacionados à informática. Nos Estados Unidos, começaram a surgir na imprensa e na literatura científica os primeiros relatos de uso de computadores para cometer delitos como sabotagem e espionagem (Barros, 2006). Em 1967, um incidente na IBM demonstrou a vulnerabilidade dos sistemas da época: estudantes convidados a testar um novo computador conseguiram explorar o sistema e "bombardeá-lo", um dos primeiros exemplos de hacking ético que levou ao desenvolvimento de medidas de segurança (Borges, 2024).

A década de 1970 foi um período de transição, com o início de estudos sistemáticos sobre o tema. Em 1972, um projeto de pesquisa na ARPANET, a precursora da internet, deu origem ao primeiro vírus, o "*Creeper*", um programa que se movia pela rede exibindo a mensagem "*I'm the creeper, catch me if you can*". Em resposta, foi criado o "Reaper", o primeiro programa antivírus, que

caçava e eliminava o *Creeper* (Borges, 2024).

A década de 1980 marcou a intensificação das ações criminosas no ambiente digital. A popularização dos computadores pessoais e o crescimento da conectividade ampliaram o campo de atuação dos criminosos. As principais modalidades de crimes envolviam a manipulação de dados bancários, a pirataria de software e os abusos nas telecomunicações (Barros, 2006).

Um dos casos mais emblemáticos da época foi o de Kevin Mitnick, que em 1979, aos 16 anos, invadiu os sistemas da Digital Equipment Corporation e copiou o software da empresa. A figura do hacker ganhou notoriedade na cultura popular com o lançamento do filme "War Games" em 1983, que retratava um jovem que quase inicia uma guerra nuclear ao invadir um sistema militar. Em 1986, o hacker alemão Marcus Hess invadiu centenas de computadores militares dos EUA, incluindo sistemas do Pentágono, com a intenção de vender informações para a KGB, evidenciando o potencial da espionagem cibernética (Borges, 2024).

O primeiro caso documentado de crime cibernético no Brasil ocorreu em 1997, quando uma jornalista passou a receber ameaças e teve seus dados pessoais expostos na internet. Este caso pioneiro evidenciou a vulnerabilidade dos usuários brasileiros no ambiente digital e a necessidade de desenvolvimento de mecanismos legais específicos para lidar com essas novas formas de criminalidade (Cazaroti, 2021).

Durante os anos 1990 e início dos anos 2000, os crimes cibernéticos no Brasil eram predominantemente caracterizados por fraudes eletrônicas simples, invasões de sistemas com motivações curiosas ou vandálicas, e a disseminação de vírus de computador. A falta de legislação específica e a limitada capacidade técnica das autoridades policiais tornavam a investigação e punição desses crimes extremamente desafiadoras.

1.2 IMPACTO DO AVANÇO TECNOLÓGICO NO SURGIMENTO DE NOVAS MODALIDADES CRIMINOSAS

A transição de uma sociedade analógica para uma sociedade digital alterou a natureza dos bens jurídicos a serem protegidos. Se antes o foco estava em bens tangíveis, como propriedades e dinheiro, hoje a proteção de dados

pessoais, informações sensíveis e ativos digitais tornou-se uma prioridade. O ciberespaço, um ambiente imaterial e sem fronteiras, tornou-se o novo palco para a prática de crimes, o que impõe desafios significativos para a aplicação da lei, especialmente no que diz respeito à jurisdição e à cooperação internacional (Borges, 2024).

O *hacking* e o roubo de dados tornaram-se mais sofisticados, com ataques direcionados a grandes corporações e governos. As fraudes eletrônicas, como o *phishing* e a engenharia social, evoluíram, utilizando técnicas cada vez mais convincentes para enganar as vítimas. O surgimento dos criptoativos, como o Bitcoin, criou um novo ecossistema para a lavagem de dinheiro e o financiamento de atividades ilícitas, devido ao alto grau de anonimato que oferecem (Borges, 2024).

A Inteligência Artificial (IA) também tem sido utilizada para fins criminosos. Os *deepfakes,* vídeos ou áudios falsificados por IA, representam uma ameaça crescente, com o potencial de serem usados para cometer fraudes, difamação e extorsão. Além disso, a crescente automação de processos levanta questões sobre a responsabilidade legal por danos causados por algoritmos autônomos (Borges, 2024).

Outro grande desafio na investigação de crimes cibernéticos é a identificação da origem do ataque e do autor do crime. O uso de técnicas de anonimização, como redes privadas virtuais (VPNs) e a rede Tor, dificulta o rastreamento dos criminosos. Além disso, a natureza global da internet permite que os ataques sejam lançados de qualquer parte do mundo, o que complica a identificação e a responsabilização dos autores (Costa; Bezerra, 2024).

O Direito tem se esforçado para acompanhar o ritmo acelerado da evolução tecnológica. No Brasil, marcos legais como o Marco Civil da Internet (Lei nº 12.965/2014), a Lei Geral de Proteção de Dados (LGPD) (Lei nº 13.709/2018) e o Marco Legal dos Criptoativos (Lei nº 14.478/2022) representam tentativas de regulamentar o ambiente digital e proteger os direitos dos cidadãos. No entanto, a natureza dinâmica dos crimes cibernéticos exige uma constante atualização da legislação e uma abordagem proativa, que antecipe as novas ameaças em vez de apenas reagir a elas.

A investigação de crimes cibernéticos apresenta uma série de desafios que a distinguem da investigação de crimes tradicionais. A natureza volátil e

transnacional das evidências digitais, a rápida evolução das tecnologias e a necessidade de conhecimentos técnicos especializados são apenas alguns dos obstáculos enfrentados pelas autoridades. Esta seção aborda os principais desafios na investigação digital, dividindo-os em técnicos, regulatórios e institucionais.

CAPÍTULO II
DESAFIOS DA INVESTIGAÇÃO DIGITAL

2.1 A INVESTIGAÇÃO DIGITAL

A crescente dependência da tecnologia digital tem sido acompanhada por um aumento significativo nos crimes cibernéticos, que abrangem um espectro diversificado de atividades ilícitas realizadas na esfera digital (Andrade, 2024). Neste contexto, a investigação digital emergiu como um campo fundamental para a aplicação da justiça, enfrentando desafios únicos que vão desde a complexidade técnica das evidências eletrônicas até questões legais e procedimentais específicas do ambiente virtual.

A forense digital, definida como um campo interdisciplinar que abrange a coleta, preservação, análise e apresentação de evidências eletrônicas, tornou-se um elemento crítico na investigação e combate aos crimes digitais (Andrade, 2024). Diferentemente das investigações tradicionais, onde as evidências físicas são tangíveis e relativamente estáveis, as evidências digitais apresentam características peculiares que exigem metodologias específicas e conhecimento técnico especializado. Rodrigues e Foltran Junior (2010) destacam que "a Forense Computacional é uma área que tem recebido significativa atenção atualmente" (2010, p.62), enfatizando a necessidade de ferramentas e técnicas adequadas para a análise de dispositivos eletrônicos e sistemas computacionais.

Os desafios enfrentados na investigação digital são multifacetados e em constante evolução, refletindo o ritmo acelerado das inovações tecnológicas. Vieira e Santos observam que "a argumentação jurídica agora depende de ferramentas e provas digitais" (2025, p.37), evidenciando a transformação fundamental que as tecnologias digitais trouxeram para o processo investigativo. Esta nova realidade exige não apenas adaptações técnicas, mas também mudanças estruturais nos procedimentos legais, na capacitação de profissionais e na cooperação entre diferentes instituições e países.

Um dos principais desafios na investigação digital reside na natureza complexa e volátil das evidências eletrônicas. Diferentemente das evidências físicas tradicionais, os dados digitais podem ser facilmente alterados, corrompidos ou destruídos, exigindo procedimentos rigorosos de preservação e

análise. Queiroz e Vargas (2010) enfatizam que a perícia forense digital deve seguir metodologias específicas para garantir a integridade e autenticidade das evidências coletadas, processo que envolve desde a identificação inicial dos dispositivos até a apresentação dos resultados em tribunal.

A volatilidade dos dados representa um desafio particular, uma vez que informações cruciais podem ser perdidas rapidamente se não forem adequadamente preservadas. Rodrigues e Foltran Junior destacam que "além de noções de Forense e Anti-forense Computacional" (2010, p.12), é necessário compreender as técnicas utilizadas por criminosos para ocultar ou destruir evidências digitais. Este aspecto da investigação exige não apenas conhecimento técnico avançado, mas também rapidez na resposta e capacidade de adaptação a novas tecnologias e métodos de ocultação.

A diversidade de dispositivos e sistemas operacionais adiciona outra camada de complexidade à investigação digital. Cada tipo de dispositivo - computadores, smartphones, tablets, dispositivos IoT - possui características específicas de armazenamento e funcionamento que requerem ferramentas e técnicas particulares de análise. Andrade (2024) observa que "com a evolução da inteligência artificial e da Internet das Coisas (IoT), os riscos cibernéticos continuarão a crescer", indicando que os investigadores devem estar constantemente atualizados com as novas tecnologias emergentes.

O volume crescente de dados também representa um desafio significativo para os investigadores. Com dispositivos de armazenamento cada vez maiores e a proliferação de serviços em nuvem, a quantidade de informações que deve ser analisada em uma investigação pode ser esmagadora. Este cenário exige não apenas ferramentas computacionais avançadas para processamento de grandes volumes de dados, mas também metodologias eficientes para filtrar e identificar informações relevantes para a investigação.

A investigação digital enfrenta desafios significativos no âmbito legal e normativo, especialmente no que se refere à admissibilidade de provas digitais e à adequação dos procedimentos jurídicos à era digital. Vieira e Santos (2025) destacam que existe "a necessidade de adaptar procedimentos jurídicos à era digital, especialmente no tocante à admissibilidade de provas digitais, através do exame de sua integridade e autenticidade". Esta adaptação é fundamental para garantir que as evidências coletadas digitalmente sejam aceitas pelos tribunais

e possam efetivamente contribuir para a aplicação da justiça.

A cadeia de custódia das evidências digitais representa um aspecto crucial que diferencia a investigação digital das práticas tradicionais. Vieira e Santos (2025) enfatizam que é necessário "visualizar a cadeia de custódia como crucial para garantir a autenticidade e integridade das evidências, especialmente no contexto das provas digitais". Este processo envolve a documentação detalhada de cada etapa da coleta, preservação, análise e apresentação das evidências, garantindo que não houve alteração ou contaminação dos dados durante o processo investigativo.

No contexto brasileiro, Andrade (2024) identifica que "a legislação cibernética brasileira enfrenta desafios na adaptação às evoluções tecnológicas e às crescentes ameaças, incluindo questões pendentes como a definição de penas para diferentes tipos de ataques e regulamentação". Esta defasagem legislativa cria incertezas jurídicas que podem comprometer a eficácia das investigações e a punição adequada dos crimes digitais. A necessidade de harmonização entre as leis nacionais e os padrões internacionais também se apresenta como um desafio, especialmente considerando a natureza transnacional de muitos crimes cibernéticos.

A questão da privacidade e proteção de dados adiciona outra dimensão aos desafios legais da investigação digital. O equilíbrio entre a necessidade de investigar crimes e o direito fundamental à privacidade dos cidadãos requer marcos legais claros e procedimentos que garantam o uso proporcional e adequado das ferramentas de investigação digital. Este aspecto é particularmente relevante no contexto da Lei Geral de Proteção de Dados (LGPD) e outras regulamentações similares que estabelecem limites para o tratamento de dados pessoais.

A investigação digital exige profissionais altamente especializados, capazes de compreender tanto os aspectos técnicos quanto os procedimentos legais envolvidos na coleta e análise de evidências eletrônicas. Andrade (2024) observa que "o sistema judiciário muitas vezes é lento na resolução de casos cibernéticos, carecendo de especialização em tecnologia e cibersegurança". Esta carência de especialização representa um gargalo significativo na eficácia das investigações digitais, limitando a capacidade das instituições de responder adequadamente aos crimes cibernéticos.

A formação de peritos em forense digital requer conhecimentos multidisciplinares que abrangem desde programação e redes de computadores até direito processual penal e criminalística. Rodrigues e Foltran Junior (2010) destacam a importância de compreender não apenas as ferramentas forenses, mas também as técnicas de "anti-forense computacional" utilizadas por criminosos para ocultar evidências. Esta necessidade de conhecimento abrangente torna o processo de capacitação longo e complexo, exigindo investimentos significativos em educação e treinamento continuado.

A velocidade das mudanças tecnológicas representa um desafio adicional para a capacitação profissional. Andrade (2024) enfatiza que "o avanço constante da tecnologia apresenta desafios técnicos, exigindo a constante atualização de métodos e ferramentas de segurança". Os profissionais da área devem estar em constante aprendizado, acompanhando as inovações tecnológicas e as novas modalidades de crimes digitais que surgem continuamente.

A escassez de recursos humanos qualificados também se reflete na distribuição desigual de capacidades investigativas entre diferentes regiões e instituições. Enquanto grandes centros urbanos podem contar com equipes especializadas em crimes cibernéticos, muitas localidades carecem de profissionais com conhecimento adequado para conduzir investigações digitais básicas. Esta disparidade pode comprometer a eficácia do sistema de justiça criminal como um todo, criando lacunas na capacidade de investigação que podem ser exploradas por criminosos.

Os crimes digitais frequentemente transcendem fronteiras nacionais, criando desafios únicos para a investigação e persecução criminal. A natureza global da internet permite que criminosos operem a partir de qualquer local do mundo, atacando vítimas em diferentes países e utilizando infraestruturas tecnológicas distribuídas geograficamente. Andrade (2024) destaca que “as cooperações internacionais são cruciais para enfrentar esse desafio em constante mudança", enfatizando a necessidade de mecanismos eficazes de colaboração entre diferentes jurisdições.

A diversidade de sistemas legais e procedimentos investigativos entre países representa um obstáculo significativo para a cooperação internacional em casos de crimes digitais. Diferentes países possuem legislações distintas sobre

crimes cibernéticos, procedimentos de coleta de evidências e mecanismos de assistência jurídica mútua, criando complexidades que podem retardar ou inviabilizar investigações transnacionais. A harmonização de procedimentos e a criação de protocolos padronizados de cooperação são essenciais para superar esses obstáculos.

A questão da soberania digital e da proteção de dados nacionais adiciona outra camada de complexidade à cooperação internacional. Muitos países implementaram regulamentações que restringem o compartilhamento de dados com autoridades estrangeiras, mesmo em contextos investigativos legítimos. Estas restrições, embora justificadas pela necessidade de proteger a privacidade dos cidadãos e a segurança nacional, podem criar barreiras para investigações de crimes que afetam múltiplas jurisdições.

A velocidade requerida nas investigações digitais também colide com os procedimentos tradicionais de cooperação jurídica internacional, que frequentemente envolvem processos burocráticos longos e complexos. Enquanto evidências digitais podem ser rapidamente destruídas ou alteradas, os mecanismos formais de assistência jurídica podem levar meses ou anos para produzir resultados. Esta discrepância temporal representa um desafio fundamental que requer o desenvolvimento de procedimentos expeditos de cooperação para casos urgentes.

CAPÍTULO III
LEGISLAÇÃO APLICÁVEL

3.1 ANÁLISE DO MARCO CIVIL DA INTERNET

O Marco Civil da Internet (MCI), Lei nº 12.965, de 23 de abril de 2014, é considerado um marco legal para o uso da internet no Brasil. Ele estabelece princípios, garantias, direitos e deveres para o uso da rede no país, além de determinar as diretrizes para a atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria (BRASIL, 2014a). A lei surgiu da necessidade de regulamentar o ambiente digital, que crescia exponencialmente e carecia de normas claras para proteger os usuários e garantir a liberdade de expressão.

Entre os princípios fundamentais do MCI, destacam-se o respeito à liberdade de expressão, a proteção da privacidade e dos dados pessoais, a preservação da neutralidade de rede e a responsabilização dos agentes de acordo com suas atividades. O art. 3º da lei elenca expressamente esses fundamentos: “A disciplina do uso da internet no Brasil tem como princípios: I – a garantia da liberdade de expressão, comunicação e manifestação de pensamento; II – a proteção da privacidade; III – a proteção dos dados pessoais, na forma da lei; IV – a preservação e garantia da neutralidade de rede; V – a preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas; VI – a responsabilização dos agentes de acordo com suas atividades; e VII – a preservação da natureza participativa da rede” (Brasil, 2014a).

A neutralidade de rede, em particular, é um dos pilares do MCI. Conforme o art. 9º, “o responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação” (Brasil, 2014a). Isso significa que os provedores de conexão não podem, por exemplo, priorizar o tráfego de determinados serviços em detrimento de outros, assegurando um ambiente de igualdade para todos os usuários e aplicações.

O MCI também aborda a questão da privacidade e da proteção dos

dados pessoais. O art. 7º assegura ao usuário que “o acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: I – inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação; II – inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei; III – inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial; IV – não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei” (Brasil, 2014a).

Outro ponto relevante do Marco Civil da Internet, regulamentado pela Lei 12.965/2014, é a responsabilização dos provedores de aplicações por conteúdos gerados por terceiros. O art. 19 dispõe que “com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente” (Brasil, 2014a). Essa regra busca equilibrar a liberdade de expressão com a necessidade de combater abusos e ilícitos na rede.

Cabe assinalar que o referido diploma legal prevê diretrizes para a atuação do poder público em relação ao uso da internet. O art. 24 estabelece que:

> A atuação da União, dos Estados, do Distrito Federal e dos Municípios, no exercício de suas competências, e em colaboração com a sociedade, o setor empresarial e a academia, será regida pelos seguintes princípios:
> I – reconhecimento da escala mundial da rede;
> II – preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;
> III – interoperabilidade entre aplicações e terminais;
> IV – incentivo à inovação e à difusão de novas tecnologias e modelos de uso e acesso;
> V – promoção da adesão a padrões tecnológicos abertos que permitam a comunicação, a acessibilidade e a interoperabilidade entre aplicações e bases de dados” (Brasil, 2014a).

O art. 25 complementa esse aspecto ao determinar que

> “as iniciativas públicas de fomento à cultura digital e de promoção da internet como ferramenta social devem:
> I – promover a inclusão digital;
> II – buscar reduzir as desigualdades, sobretudo entre as diferentes regiões do País, no acesso às tecnologias da informação e comunicação e no seu uso;
> III – fomentar a produção e circulação de conteúdo nacional;
> IV – desenvolver ações e programas de capacitação para o uso da internet;
> V – promover a diversidade cultural e linguística;
> VI – promover a produção e circulação de conteúdo nacional” (BRASIL, 2014a).

O art. 26 ainda destaca a importância da educação digital, prevendo que “o Estado deve, periodicamente, formular e fomentar estudos, inclusive comparativos, sobre a gestão da rede mundial de computadores, bem como sobre a relação entre a internet e a cidadania” (Brasil, 2014a).

Em seus dez anos de vigência, o Marco Civil da Internet tem sido fundamental para garantir os direitos dos usuários e moldar o ambiente digital brasileiro. No entanto, novos desafios surgem com o avanço tecnológico, como a inteligência artificial e a disseminação de notícias falsas, o que tem levado a discussões sobre a necessidade de aprimoramento da legislação (SENADO FEDERAL, 2024).

3.2 ANÁLISE DA LEI CAROLINA DIECKMANN

A Lei nº 12.737, de 30 de novembro de 2012, popularmente conhecida como Lei Carolina Dieckmann, representa um marco na legislação brasileira ao tipificar crimes cibernéticos. A lei foi sancionada em resposta a um incidente de grande repercussão envolvendo a atriz Carolina Dieckmann, que teve fotos íntimas divulgadas na internet após a invasão de seus dispositivos eletrônicos (Brasil, 2012).

Antes da Lei Carolina Dieckmann, o Código Penal brasileiro não possuía dispositivos específicos para lidar com crimes cometidos no ambiente digital, o que gerava uma lacuna legal e dificultava a punição de infratores. A nova legislação alterou o Código Penal para incluir o artigo 154-A, que criminaliza a invasão de dispositivo informático alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar

vulnerabilidades para obter vantagem ilícita (Brasil, 2012).

O art. 154-A, inserido no Código Penal, é seu principal marco: “Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena – detenção, de 3 (três) meses a 1 (um) ano, e multa” (Brasil, 2012).

O §1º criminaliza a produção e difusão de ferramentas de invasão: “Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput” (Brasil, 2012).

O §2º prevê hipóteses qualificadas: “Aumenta-se a pena de um sexto a um terço se da invasão resulta a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido” (Brasil, 2012).

Já o §3º acrescenta: “Se da invasão resultar prejuízo econômico, a pena é aumentada de um terço a dois terços” (Brasil, 2012).

O §4º trata da divulgação ilícita: “Na hipótese do §2º, se houver divulgação, comercialização ou transmissão a terceiro, a pena é de reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, sem prejuízo da pena correspondente à violência” (Brasil, 2012).

Outro dispositivo importante é o art. 266 do Código Penal, que ganhou o §1º-A: “Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública” (Brasil, 2012). Esse artigo passou a enquadrar ataques de negação de serviço (DoS e DDoS), comuns no ambiente digital.

A lei também modificou o art. 298 do Código Penal, que trata da falsificação de documento particular, passando a incluir expressamente “cartão de crédito ou débito” como documento sujeito à falsificação penalmente relevante (Brasil, 2012).

A lei buscou, assim, oferecer um amparo legal mais robusto para combater a crescente onda de crimes digitais que afetavam a privacidade e a segurança dos usuários da internet (SENADO FEDERAL, 2023).

Apesar de sua importância, a Lei Carolina Dieckmann foi alvo de

algumas críticas, principalmente em relação à sua abrangência e à necessidade de aprimoramento para acompanhar a rápida evolução tecnológica. No entanto, é inegável que a lei representou um avanço significativo na proteção da privacidade e no combate aos crimes cibernéticos no Brasil, servindo como um importante instrumento para coibir práticas ilícitas no ambiente virtual (DEFENSORIA PÚBLICA DO CEARÁ, 2022).

É importante ressaltar que a Lei Carolina Dieckmann, embora focada em crimes cibernéticos, pavimentou o caminho para discussões mais amplas sobre a proteção de dados pessoais, que culminariam na criação da Lei Geral de Proteção de Dados (LGPD). Ambas as leis, embora com escopos distintos, compartilham o objetivo de garantir a segurança e a privacidade dos usuários no ambiente digital (BFBM, [s.d.]).

3.3 DISCUSSÃO SOBRE A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709, de 14 de agosto de 2018, representa um divisor de águas na forma como os dados pessoais são tratados no Brasil. Inspirada no Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, a LGPD estabelece um conjunto de regras para a coleta, uso, armazenamento e compartilhamento de dados pessoais, tanto em meios físicos quanto digitais, por pessoas físicas ou jurídicas de direito público ou privado (BRASIL, 2018).

O principal objetivo da LGPD é proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Nesse sentido, o art. 1º da lei dispõe: *“Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural”* (Brasil, 2018).

Para isso, a lei define no art. 5º, I, que dados pessoais são *“informação relacionada a pessoa natural identificada ou identificável”*. Já os dados pessoais sensíveis são definidos no art. 5º, II, como *“dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida*

sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural" (Brasil, 2018).

Entre os princípios que regem o tratamento de dados pessoais, o art. 6º da LGPD estabelece:

> As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
> I – finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular;
> II – adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
> III – necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades;
> IV – livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
> V – qualidade dos dados;
> VI – transparência;
> VII – segurança;
> VIII – prevenção;
> IX – não discriminação;
> X – responsabilização e prestação de contas (Brasil, 2018*)*.

Outro ponto fundamental é o conjunto de bases legais do tratamento de dados. O art. 7º determina que:

> [...] o tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> I – mediante o fornecimento de consentimento pelo titular;
> II – para o cumprimento de obrigação legal ou regulatória;
> III – pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas;
> IV – para a realização de estudos por órgão de pesquisa;
> V – quando necessário para a execução de contrato ou de procedimentos preliminares;
> VI – para o exercício regular de direitos em processo judicial, administrativo ou arbitral;
> VII – para a proteção da vida ou da incolumidade física do titular ou de terceiro;
> VIII – para a tutela da saúde;
> IX – para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular" (Brasil, 2018).

A LGPD também criou a Autoridade Nacional de Proteção de Dados (ANPD). O art. 55-A define que *"fica criada, sem aumento de despesa, a Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal, integrante da Presidência da República"* (BRASIL, 2018). Compete à ANPD, conforme o art. 55-J, *"zelar pela proteção dos dados pessoais, elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da*

Privacidade, fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação".

As sanções estão previstas no art. 52:

> Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela ANPD:
> I – advertência;
> II – multa simples de até 2% do faturamento da pessoa jurídica, limitada a R$ 50.000.000,00 por infração;
> III – multa diária;
> IV – publicização da infração;
> V – bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
> VI – eliminação dos dados pessoais a que se refere a infração;
> VII – suspensão parcial do funcionamento do banco de dados;
> VIII – suspensão do exercício da atividade de tratamento;
> IX – proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados (Brasil, 2018).

A entrada em vigor da LGPD, em setembro de 2020, exigiu que empresas e órgãos públicos revisassem suas práticas de tratamento de dados, implementando medidas de segurança e governança para garantir a conformidade com a lei. A LGPD representa um avanço significativo na proteção da privacidade dos cidadãos brasileiros, conferindo-lhes maior controle sobre suas informações pessoais e promovendo um ambiente digital mais seguro e transparente (SENADO FEDERAL, 2020).

CAPÍTULO IV
ANÁLISE DA EFICÁCIA DAS MEDIDAS LEGAIS

Os crimes cibernéticos, que abrangem desde fraudes online e roubo de dados até ataques a infraestruturas críticas, representam um desafio complexo para os sistemas jurídicos em todo o mundo. No Brasil, a legislação tem buscado se adaptar a essa realidade dinâmica, com a promulgação de leis específicas e a atualização de marcos legais existentes. Com a Lei Geral de Proteção de Dados (LGPD), o Brasil avançou significativamente na regulamentação do tratamento de dados, impondo responsabilidades às empresas e garantindo direitos aos titulares. A violação desses dados, muitas vezes por meio de ataques cibernéticos, pode gerar sanções administrativas e civis, além das implicações penais. A LGPD, portanto, atua como uma medida legal complementar no combate aos crimes cibernéticos, ao estabelecer um padrão de segurança e responsabilização que visa prevenir incidentes (Brasil, 2018).

4.1 AVANÇOS OBTIDOS COM A LEGISLAÇÃO EXISTENTE

A legislação brasileira tem demonstrado um esforço contínuo para se adaptar aos desafios impostos pelos crimes cibernéticos, resultando em avanços significativos. O marco inicial e mais conhecido é a Lei nº 12.737/2012, popularmente conhecida como Lei Carolina Dieckmann. Esta lei tipificou condutas como a invasão de dispositivo informático, interrupção ou perturbação de serviço telemático ou de informação, e falsificação de cartão de crédito ou débito. Embora tenha sido um passo importante, sua abrangência foi considerada limitada por muitos especialistas (Brasil, 2012).

Posteriormente, a Lei nº 14.155/2021 trouxe alterações importantes ao Código Penal, aumentando as penas para crimes de furto e estelionato cometidos de forma eletrônica ou pela internet. Essa lei também criou o crime de fraude eletrônica, com penas mais severas quando praticado mediante a utilização de servidores mantidos fora do país ou em larga escala. Esses avanços refletem a necessidade de uma resposta mais robusta do Estado diante do crescimento exponencial das fraudes digitais (Brasil, 2021).

Além das leis específicas, outras normativas e marcos legais contribuem para o enfrentamento dos crimes cibernéticos. A Lei nº 9.296/96, que regulamenta a interceptação de comunicações telefônicas e de sistemas de informática e telemática, é uma ferramenta essencial para a investigação desses delitos, permitindo a coleta de provas digitais. A Lei do Marco Civil da Internet (Lei nº 12.965/2014) estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil, incluindo a previsão de guarda de registros de conexão e acesso a aplicações, que são fundamentais para a rastreabilidade de atividades criminosas online (Brasil, 1996; Brasil, 2014).

Os avanços não se limitam apenas à tipificação de condutas e ao aumento de penas. Há também um movimento para o aprimoramento das capacidades investigativas e de persecução penal. A criação de delegacias especializadas em crimes cibernéticos e a capacitação de peritos digitais são exemplos de iniciativas que visam fortalecer a resposta do Estado. A cooperação internacional também tem se mostrado um pilar fundamental, dada a natureza transnacional dos crimes cibernéticos, com acordos e tratados que facilitam a troca de informações e a colaboração entre países.

4.2 IDENTIFICAÇÃO DE LACUNAS E A NECESSIDADE DE ATUALIZAÇÕES CONSTANTES

O surgimento de novas tecnologias continua a criar desafios inéditos para a investigação digital, exigindo adaptação constante das metodologias e ferramentas utilizadas pelos investigadores. Vieira e Santos (2025) observam que as tecnologias preditivas e a inteligência artificial estão sendo incorporadas às práticas investigativas, mas alertam sobre "os riscos da aplicação indiscriminada dessas abordagens". O uso de algoritmos de reconhecimento facial, análise preditiva e outras ferramentas baseadas em IA pode introduzir vieses e erros que comprometem a qualidade das investigações.

A criptografia representa um desafio particular para a investigação digital, criando um dilema entre a necessidade de proteger a privacidade e a segurança dos dados e a capacidade das autoridades de investigar crimes. Dispositivos e comunicações cada vez mais criptografados podem tornar impossível o acesso a evidências cruciais, mesmo com autorização judicial

adequada. Este cenário exige o desenvolvimento de abordagens equilibradas que preservem tanto a segurança digital quanto a capacidade investigativa das autoridades.

A proliferação de dispositivos conectados à Internet das Coisas (IoT) cria novos vetores de evidências digitais, mas também novos desafios técnicos e legais. Andrade (2024) destaca que "com a evolução da inteligência artificial e da Internet das Coisas (IoT), os riscos cibernéticos continuarão a crescer". Estes dispositivos frequentemente possuem capacidades limitadas de logging e forense, além de questões complexas de propriedade e acesso aos dados que geram.

As tecnologias de blockchain e criptomoedas introduzem desafios adicionais relacionados ao anonimato e à rastreabilidade de transações financeiras. Embora estas tecnologias não sejam inerentemente anônimas, elas requerem conhecimentos especializados e ferramentas específicas para investigação, além de levantarem questões sobre a regulamentação e supervisão de ativos digitais.

CAPÍTULO V
PERSPECTIVAS FUTURAS

5.1 A INFLUÊNCIA DA INTELIGÊNCIA ARTIFICIAL NA SEGURANÇA DIGITAL

A Inteligência Artificial (IA) surgiu como uma força transformadora em diversos setores, e a segurança digital não é exceção. Sua capacidade de processar e analisar grandes volumes de dados em tempo real, identificar padrões complexos e automatizar respostas a ameaças tem revolucionado a forma como as organizações se defendem contra os ataques cibernéticos. Uma das principais contribuições da IA para a segurança digital é aprimorar a detecção de ameaças. Algoritmos de aprendizado de máquina podem analisar o tráfego de rede, logs de sistemas e comportamentos de usuários para identificar anomalias que indicam a presença de malware, tentativas de *phishing*, ataques de *ransomware* ou outras atividades maliciosas. Diferente dos sistemas de segurança tradicionais baseados em assinaturas, que dependem de ameaças conhecidas, a IA pode detectar ameaças novas e sofisticadas, incluindo ataques de dia zero, ao reconhecer padrões incomuns que fogem ao comportamento normal.

A influência da IA na segurança digital não se restringe apenas aos benefícios para a defesa. A mesma tecnologia que fortalece as defesas pode ser utilizada por cibercriminosos para orquestrar ataques mais sofisticados e em larga escala. A IA pode ser empregada para desenvolver malwares mais inteligentes e evasivos, criar campanhas de *phishing* altamente personalizadas (*spear phishing*) e automatizar a busca por vulnerabilidades em sistemas. A evolução de modelos de IA autônomos, capazes de planejar e executar ataques sem intervenção humana, representa um cenário preocupante para o futuro da cibersegurança (Cuenca, 2024).

5.2 TENDÊNCIAS LEGISLATIVAS PARA ENFRENTAR NOVOS DESAFIOS TECNOLÓGICOS

O ritmo acelerado da inovação tecnológica, especialmente no campo da Inteligência Artificial, impõe um desafio constante aos legisladores: como criar

um arcabouço legal que seja eficaz na proteção da sociedade contra os crimes cibernéticos, sem sufocar o desenvolvimento tecnológico? As tendências legislativas atuais refletem essa busca por equilíbrio, focando na adaptação das leis existentes, na criação de novas regulamentações e na promoção da cooperação internacional.

Uma das principais tendências é a harmonização legislativa e a outra é a regulamentação específica da Inteligência Artificial. À medida que a IA se torna mais presente em diversas áreas, surgem preocupações sobre seu uso ético, a proteção de dados e o potencial para ser utilizada em atividades criminosas. Propostas legislativas em vários países, incluindo o Brasil, buscam estabelecer diretrizes para o desenvolvimento e uso responsável da IA, abordando questões como transparência, explicabilidade dos algoritmos, responsabilidade por danos causados por sistemas de IA e a exigência de avaliações de segurança (Soares 2025; Cuenca, 2024). O objetivo é criar um ambiente regulatório que fomente a inovação, mas que também proteja os direitos fundamentais e a segurança digital dos cidadãos.

A União Europeia lidera esta tendência com o AI Act (Regulamento 2024/1689), que entrou em vigor em agosto de 2024, estabelecendo o primeiro marco regulatório abrangente para inteligência artificial no mundo. O regulamento europeu classifica os sistemas de IA em categorias de risco: aplicações que criam risco inaceitável são proibidas, sistemas de alto risco estão sujeitos a requisitos legais específicos, enquanto aplicações não explicitamente proibidas ou listadas como de alto risco permanecem amplamente não regulamentadas (LANTYER, 2023).

A LGPD no Brasil é um exemplo de como a legislação busca empoderar os indivíduos sobre seus dados e impor responsabilidades às organizações. As tendências futuras apontam para um fortalecimento dessas normativas, com maior fiscalização e sanções mais rigorosas para o descumprimento, especialmente em um cenário onde a coleta e o processamento de dados são intensificados pela IA. A legislação busca se adaptar aos novos tipos de crimes cibernéticos que surgem com a evolução tecnológica. Isso inclui a tipificação de condutas relacionadas a deepfakes, manipulação de informações por IA, crimes em metaversos e outras formas emergentes de cibercriminalidade. A agilidade legislativa é um desafio, mas a colaboração entre especialistas em tecnologia, direito e segurança é fundamental para garantir que as leis possam acompanhar

a complexidade e a velocidade das ameaças digitais (Cuenca, 2024).

Com a natureza transnacional dos crimes cibernéticos, a fragmentação de leis entre diferentes países dificulta a persecução penal e a cooperação entre as autoridades. Iniciativas para criar padrões e acordos internacionais que facilitem a troca de informações, a extradição de criminosos e a aplicação de sanções são cruciais.

5.3 EXPERIÊNCIAS INTERNACIONAIS DE LEGISLAÇÕES MAIS RIGOROSAS

A eficácia das legislações nacionais depende crescentemente de mecanismos robustos de cooperação internacional. A recente aprovação da Convenção das Nações Unidas sobre Crimes Cibernéticos, em dezembro de 2024, representa um marco na harmonização global de esforços de combate ao cibercrime (NAÇÕES UNIDAS, 2024). Esta convenção complementa a Convenção de Budapeste, ampliando o escopo de cooperação internacional e estabelecendo novos mecanismos para o combate a crimes cibernéticos transnacionais.

- Singapura: Modelo de Rigor Legislativo

  Singapura representa um exemplo de jurisdição com legislação particularmente rigorosa em crimes cibernéticos. O Computer Misuse Act de Singapura, atualizado em 2023, estabelece penas severas para crimes cibernéticos, incluindo prisão de até 20 anos para ataques a infraestruturas críticas. A legislação singapurense também criminaliza especificamente a posse de ferramentas de hacking e estabelece responsabilidade criminal para administradores de sistemas que não implementem medidas de segurança adequadas (Singapure, 2023).

- China: Regulamentação Abrangente de IA e Cibersegurança

  A China adotou uma abordagem abrangente para a regulamentação de IA e cibersegurança. A Lei de Segurança Cibernética da China, em vigor desde 2017, estabelece requisitos rigorosos para operadores de infraestruturas críticas e exige a localização de dados dentro do território chinês. Adicionalmente, as Regulamentações sobre Algoritmos de Recomendação, implementadas em 2022, estabelecem controles específicos sobre

o uso de algoritmos de IA por empresas de tecnologia (China, 2017).

- Reino Unido: Online Safety Act

  O Reino Unido aprovou em 2023 o Online Safety Act, uma das legislações mais abrangentes do mundo para regulamentação de conteúdo online e segurança digital A lei estabelece obrigações específicas para plataformas digitais removerem conteúdo ilegal e protegerem usuários, especialmente crianças, com multas que podem chegar a 10% do faturamento anual global das empresas. (Reino Unido, 2023)

Como observa Fernandes (2025), a harmonização normativa e a colaboração entre diferentes jurisdições são essenciais para enfrentar eficazmente os desafios impostos pela criminalidade digital

Os principais desafios para o desenvolvimento de legislações eficazes em crimes cibernéticos incluem:

(1) a velocidade da evolução tecnológica, que frequentemente supera a capacidade de resposta legislativa;
(2) a necessidade de equilibrar inovação e proteção;
(3) a complexidade técnica que exige conhecimento especializado dos legisladores; e
(4) a natureza transnacional dos crimes digitais.

As perspectivas futuras apontam para uma maior convergência entre legislações nacionais, impulsionada pela necessidade de cooperação internacional efetiva. A tendência é de desenvolvimento de marcos regulatórios mais flexíveis e adaptativos, capazes de responder rapidamente às mudanças tecnológicas sem comprometer a segurança jurídica.

CONCLUSÃO

A crescente digitalização da sociedade e a constante evolução tecnológica trouxeram consigo um cenário complexo para o direito, especialmente no que tange aos crimes cibernéticos. A análise da eficácia das medidas legais existentes revela um esforço contínuo do legislador brasileiro em adaptar-se a essa nova realidade, com avanços significativos na tipificação de condutas e no endurecimento de penas. Leis como a Lei Carolina Dieckmann (Lei nº 12.737/2012) e as alterações promovidas pela Lei nº 14.155/2021 representam marcos importantes na tentativa de coibir práticas criminosas no ambiente digital, como a invasão de dispositivos informáticos, furtos e estelionatos eletrônicos. No entanto, a eficácia plena dessas medidas ainda é um desafio, dada a velocidade com que novas modalidades de crimes surgem e a dificuldade de investigação e persecução penal em um ambiente transnacional e muitas vezes anônimo.

A influência da Inteligência Artificial (IA) na segurança digital é um campo de dupla face. Por um lado, a IA emerge como uma ferramenta poderosa para aprimorar a detecção de ameaças, a prevenção de fraudes e a automação de respostas a incidentes cibernéticos, fortalecendo as defesas contra-ataques cada vez mais sofisticados. Sistemas de IA podem analisar grandes volumes de dados em tempo real, identificar padrões suspeitos e prever vulnerabilidades, tornando-se aliadas indispensáveis na proteção de dados e infraestruturas críticas. Por outro lado, a mesma tecnologia pode ser instrumentalizada por criminosos para desenvolver ataques mais complexos, como phishing altamente personalizado, criação de deepfakes para fraudes e manipulação de informações, e até mesmo a automação de ataques cibernéticos em larga escala. Esse dualismo exige uma abordagem cautelosa e proativa, tanto no desenvolvimento quanto na regulamentação da IA.

As tendências legislativas para enfrentar esses novos desafios tecnológicos apontam para a necessidade de uma harmonização internacional, dada a natureza sem fronteiras do ciberespaço. A regulamentação específica da IA, com foco em diretrizes éticas, transparência e responsabilidade, é uma pauta urgente para garantir o uso seguro e justo dessa tecnologia. Além disso, o fortalecimento da proteção de infraestruturas críticas e a contínua evolução das

leis de privacidade e proteção de dados, como a LGPD, são essenciais para construir um ambiente digital mais seguro e confiável. A agilidade legislativa e a colaboração multidisciplinar entre juristas, tecnólogos e especialistas em segurança são fundamentais para que o direito possa acompanhar a complexidade e a velocidade das ameaças cibernéticas, garantindo a proteção dos cidadãos e a integridade do ambiente digital.

O combate aos crimes cibernéticos é uma corrida constante contra a inovação criminosa. Embora a legislação brasileira tenha demonstrado avanços significativos, a eficácia das medidas legais depende não apenas da existência de leis robustas, mas também da capacidade de adaptação do sistema judiciário e das forças de segurança, do investimento em tecnologia e capacitação, e da cooperação internacional. A Inteligência Artificial, com seu potencial transformador, apresenta tanto oportunidades quanto riscos, exigindo uma regulamentação inteligente e flexível que promova a inovação ao mesmo tempo em que protege a sociedade. O futuro da segurança digital e da justiça no ciberespaço dependerá da nossa capacidade de antecipar, adaptar e colaborar diante dos desafios tecnológicos emergentes.

REFERÊNCIAS

ALMEIDA, J. de J. Crimes cibernéticos. Caderno de Graduação - Ciências Humanas e Sociais - UNIT, v. 3, n. 1, p. 41-52, 2015. Disponível em: https://periodicos.grupotiradentes.com/cadernohumanas/article/view/2013. Acesso em: 17 set. 2025.

ANDRADE, Ingrid Lima de. Forense digital aplicada ao combate de crimes cibernéticos: uma revisão. Revista Foco, v. 17, n. 7, p. e5771, 2024. Disponível em: https://ojs.focopublicacoes.com.br/foco/article/view/5771. Acesso em: 18 set. 2025.

BARROS, Antônio. Conheça a evolução dos crimes cibernéticos. Agência Câmara, 23/08/2006. Disponível em: https://www.camara.leg.br/noticias/89137-conheca-a-evolucao-dos-crimes-ciberneticos Acesso em: 17 set. 2025.

BELEZZI, Henrique Silva Ribeiro; ROSA, Guilherme Freire. "Os crimes cibernéticos na legislação brasileira e sua abordagem". Colloquium Socialis, v. 1, n. 2, p. 01-06, 2017. Disponível: https://journal.unoeste.br/index.php/cs/article/download/1790/1748/7139.

BFBM. **Lei Carolina Dieckmann, evolução tecnológica e LGPD: necessidade de harmonização**. [S. l.], [s.d.]. Disponível em: https://www.bfbm.com.br/lei-carolina dieckmann-evolucao-tecnologica-e-lgpd-necessidade-de-harmonizacao/. Acesso em: 10 set. 2025.

BORGES, Beatriz. Como a Era Digital Impacta o Direito e as Novas Modalidades de Crimes Cibernéticos. Blog do Direito IDP, 02 dez. 2024. Disponível em: https://pos.idp.edu.br/idp-learning/blog/direito-digital/como-a-era-digital-impacta-o-direito-e-as-novas-modalidades-de-crimes-ciberneticos/

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências. **Diário Oficial da União**, Brasília, DF, 30 nov. 2012. Disponível em:

https://www.planalto.gov.br/ccivil_03/_ato2011- 2014/2012/lei/l12737.htm. Acesso em: 10 set. 2025.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial da União**, Brasília, DF, 23 abr.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**, Brasília, DF, 14 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 set. 2025.

BRASIL. Lei nº 14.155, de 27 de maio de 2021. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para dispor sobre a competência territorial em casos de crimes cometidos de forma eletrônica ou pela internet. Diário Oficial da União, Brasília, DF, 28 maio 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019- 2022/2021/lei/L14155.htm. Acesso em: 17 set. 2025.

CARVALHO, G. M. A Eficácia da Legislação Brasileira na Prevenção de Crimes Digitais. 2024. Disponível em: https://www.jusbrasil.com.br/artigos/a-eficacia-da-legislacao brasileira-na-prevencão-de-crimes-digitais/2147918640. Acesso em: 17 set. 2025.

CAZAROTI, Tatiane Martins Barros. Crimes Cibernéticos. Repositório Digital 2014. Disponível em: https://www.repositoriodigital.univag.com.br/index.php /rep/ article/ view/203/235. Acesso em: 10 set. 2025.

CHADD, Katie. The History Of Cybercrime And Cybersecurity, 1940-2020. Cybersecurity Ventures, 30 nov. 2020. Disponível em: https://cybersecurityventures.com/the-history-of-cybercrime-and-cybersecurity-

1940-2020/

CHINA. Cybersecurity Law of the People's Republic of China. Em vigor desde 1º de junho de 2017. Disponível em: https://digichina.stanford.edu/work/translationcybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/. Acesso em: 08 jan. 2025.

COSTA, Ludymilla Sena; BEZERRA, Marco Antônio Alves. Os desafios da investigação criminal de crimes virtuais na era digital. Revista Ibero-Americana de Humanidades, Ciências e Educação, v. 10, n. 10, p. 2111-2132, 2024.

CRUZ, D.; RODRIGUES, J. Crimes cibernéticos e a falsa sensação de impunidade. Revista Científica Eletrônica do Curso de Direito, v. 16, n. 1, p. 15-28, 2018. Disponível em: https://faef.revista.inf.br/imagens_arquivos/arquivos_destaque/iegWxiOtVJB1t5C_2019-2-28-16-36-0.pdf. Acesso em: 17 set. 2025.

CUENCA, F. R. Tendências em cibersegurança 2025: uso malicioso da IA generativa e tecnologias operacionais estão no radar. 2024. Disponível em: https://www.welivesecurity.com/pt/seguranca-digital/tendencias-em-ciberseguranca- 2025-uso-malicioso-da-ia-generativa-e-tecnologias-operacionais-estao-no-radar/.

DEFENSORIA PÚBLICA DO CEARÁ. **Lei Carolina Dieckmann: 10 anos da lei que protege a privacidade dos brasileiros no ambiente virtual**. Fortaleza, 2 dez. 2022. Disponível em: https://www.defensoria.ce.def.br/noticia/lei-carolina-dieckmann-10- anos-da-lei-que-protege-a-privacidade-dos-brasileiros-no-ambiente-virtual/. Acesso em: 10 set. 2025.

FERNANDES, O. Tendências Regulatórias no Brasil: A Convergência entre Proteção de Dados, Inteligência Artificial e Segurança Cibernética. 2025. Disponível em: https://okai.com.br/blog/tendencias-regulatorias-no-brasil-a-convergencia-entre protecao-de-dados-inteligencia-artificial-e-seguranca-cibernetica. Acesso em: 17 set. 2025.

KASPERSKY. "O que é crime cibernético? Aprenda a como se proteger". Disponível em: https://www.kaspersky.com.br/resource-center/threats/what-is-cybercrime

LANTYER, Victor Hugo. Entendendo o EU AI Act: uma nova era na regulamentação da IA na Europa. Migalhas, São Paulo, 15 dez. 2023. Disponível em: https://www.migalhas.com.br/arquivos/2023/12/B6D06B89351862_Artigo-RegulamentoEuropeudeIA-.pdf. Acesso em: 18 set. 2025.

PARDINI, V. Inteligência Artificial na Segurança: confira os benefícios. 2025. Disponível em: https://www.docusign.com/pt-br/blog/inteligencia-artificial seguranca. Acesso em: 17 set. 2025.

QUEIROZ, Carlos; VARGAS, Rodrigo. Investigação e perícia forense computacional. Rio de Janeiro: Brasport, 2010.

REINO UNIDO. Online Safety Act 2023. Disponível em: https://www.legislation.gov.uk/ukpga/2023/50. Acesso em: 08 jan. 2025.

RODRIGUES, Tiago Scharr; FOLTRAN JUNIOR, Dirceu Cesar. Análise de ferramentas forenses na investigação digital. Revista Tecnológica da UEG, Anápolis, v. 1, n. 1, p. 52-67, 2010. Disponível em: https://ri.uepg.br/riuepg/handle/123456789/530. Acesso em: 18 set. 2025.

SENADO FEDERAL. **Lei Geral de Proteção de Dados entra em vigor**. Brasília, DF, 18 set. 2020. Disponível em: https://www12.senado.leg.br/noticias/materias/2020/09/18/lei-geral-de-protecao-de dados-entra-em-vigor. Acesso em: 10 set. 2025.

SENADO FEDERAL. **Marco Civil da Internet completa dez anos ante desafios sobre redes sociais e IA**. Brasília, DF, 26 abr. 2024. Disponível em: https://www12.senado.leg.br/noticias/materias/2024/04/26/marco-civil-da-internet completa-dez-anos-ante-desafios-sobre-redes-sociais-e-ia. Acesso em:

10 set. 2025.

SINGAPURA. Computer Misuse (Amendment) Act 2023. Disponível em: https://sso.agc.gov.sg/Acts-Supp/16-2023/Published/20230605?DocDate=20230605. Acesso em: 08 jan. 2025

SOARES, V. Panorama Mundial da Legislação de Inteligência Artificial. 2025. Disponível em: https://www2.camara.leg.br/a-camara/estruturaadm/secretarias/secretaria-da-inovacao-legislativa/publicacoes/panorama-mundial-da-legislacao-de-inteligencia-artificial/view. Acesso em: 17 set. 2025.

UNIVAG, 2021. Disponível em: https://www.repositoriodigital.univag.com.br/index.php/rep/article/view/203/235

UNODC - Escritório das Nações Unidas sobre Drogas e Crime. 2025. Crimes cibernéticos. Disponível em: https://www.unodc.org/lpo-brazil/pt/covid19/cibercriminalidade-e-desinformacao.html.

VIEIRA, Andrey Bruno Cavalcante; SANTOS, Hugo Leonardo Rodrigues. Investigação criminal e tecnologias digitais: algumas reflexões sobre o policiamento preditivo e a admissibilidade de provas digitais. Revista Brasileira de Direito Processual Penal, v. 11, n. 1, p. 1-30, 2025. Disponível em: https://revista.ibraspp.com.br/RBDPP/article/view/1072. Acesso em: 18 set. 2025.