UNILEÃO
CENTRO UNIVERSITÁRIO DOUTOR LEÃO SAMPAIO
CURSO DE GRADUAÇÃO EM DIREITO

PEDRO HENRIQUE GUEDES OLIVEIRA

DESAFIOS JURÍDICOS E REGULATÓRIOS DA INTELIGÊNCIA ARTIFICIAL EM CRIMES CIBERNÉTICOS: EXPLORANDO AS LACUNAS NA LEGISLAÇÃO ATUAL E PROPONDO DIRETRIZES PARA UMA REGULAÇÃO PENAL EFICAZ

JUAZEIRO DO NORTE-CE
2025

PEDRO HENRIQUE GUEDES OLIVEIRA

DESAFIOS JURÍDICOS E REGULATÓRIOS DA INTELIGÊNCIA ARTIFICIAL EM CRIMES CIBERNÉTICOS: EXPLORANDO AS LACUNAS NA LEGISLAÇÃO ATUAL E PROPONDO DIRETRIZES PARA UMA REGULAÇÃO PENAL EFICAZ

Trabalho de Conclusão de Curso – *Artigo Científico,* apresentado à Coordenação do Curso de Graduação em Direito do Centro Universitário Doutor Leão Sampaio, em cumprimento às exigências para a obtenção do grau de Bacharel.

Orientador: Francisco Gledison Lima Araújo, Bacharel em Direito pelo Centro Universitário Dr. Leão Sampaio, Mestrando em Direito Constitucional pela UNIFIEO-SP, Especialista em Direito DIigital e Nova Tecnologias do Direito - CEDIN-BH

JUAZEIRO DO NORTE-CE
2025

PEDRO HENRIQUE GUEDES OLIVEIRA

DESAFIOS JURÍDICOS E REGULATÓRIOS DA INTELIGÊNCIA ARTIFICIAL EM CRIMES CIBERNÉTICOS: EXPLORANDO AS LACUNAS NA LEGISLAÇÃO ATUAL E PROPONDO DIRETRIZES PARA UMA REGULAÇÃO PENAL EFICAZ

Este exemplar corresponde à redação final aprovada do Trabalho de Conclusão de Curso de PEDRO HENRIQUE GUEDES OLIVEIRA

Data da Apresentação _____/_____/_____

BANCA EXAMINADORA

Orientador: (TITULAÇÃO E NOME COMPLETO)

Membro: (TITULAÇÃO E NOME COMPLETO/ SIGLA DA INSTITUIÇÃO)

Membro: (TITULAÇÃO E NOME COMPLETO/ SIGLA DA INSTITUIÇÃO)

JUAZEIRO DO NORTE-CE
2025

DESAFIOS JURÍDICOS E REGULATÓRIOS DA INTELIGÊNCIA ARTIFICIAL EM CRIMES CIBERNÉTICOS: EXPLORANDO AS LACUNAS NA LEGISLAÇÃO ATUAL E PROPONDO DIRETRIZES PARA UMA REGULAÇÃO PENAL EFICAZ

Pedro Henrique Guedes Oliveira[1]
Francisco Gledison Lima Araújo[2]

RESUMO

Este estudo se debruça sobre os desafios jurídicos e regulatórios que emergem da introdução da Inteligência Artificial (IA) na esfera dos delitos cibernéticos, com uma atenção especial às lacunas presentes na legislação brasileira e à proposta de diretrizes que visem uma regulação penal eficaz. A evolução tecnológica e a autonomia crescente dos sistemas de IA têm dado origem a novas formas de criminalidade digital, como *deepfakes*, fraudes automatizadas e phishing inteligente, que desafiam as definições convencionais do Direito Penal. A revisão da legislação brasileira, incluindo a Lei n. 12.737/2012 e artigos do Código Penal, demonstra que as especificidades dos crimes mediados por algoritmos autônomos e aprendizado de máquina ainda não são adequadamente abordadas. Observou-se que a responsabilização penal enfrenta desafios significativos, especialmente na identificação do agente, na obtenção de provas digitais e na definição de autoria e dolo. Propõe-se, portanto, a criação de um marco regulatório dinâmico e multidisciplinar, em consonância com os direitos fundamentais. Recomenda-se que o Brasil adote a Convenção de Budapeste, desenvolva legislação específica para crimes cibernéticos que envolvam IA, fortaleça a cooperação internacional e invista na educação digital e na capacitação técnica dos profissionais do direito. Além disso, destaca-se a importância de o Estado utilizar a própria IA como uma ferramenta de monitoramento, investigação e prevenção, sempre respeitando as garantias constitucionais. Conclui-se que o combate aos crimes cibernéticos que utilizam inteligência artificial exige um novo paradigma jurídico, capaz de harmonizar inovação tecnológica, segurança jurídica e proteção dos direitos humanos.

Palavras-chave: Inteligência Artificial; Crimes Cibernéticos; Legislação Penal; Responsabilização; Direitos Fundamentais.

1 INTRODUÇÃO

A rápida evolução da Inteligência Artificial (IA) tem provocado uma transformação significativa em diversas áreas da sociedade, especialmente no campo da segurança digital e da legislação. A aplicação da IA, tanto em processos de proteção quanto em crimes cibernéticos, trouxe consigo uma série de desafios jurídicos e regulatórios. Com o aumento da utilização de tecnologias de IA em crimes digitais, como ataques cibernéticos, fraudes e roubo de dados, tornou-se evidente a necessidade urgente de adequar a legislação brasileira para

[1]Graduando do Curso de Direito do Centro Universitário Doutor Leão Sampaio/Unileão.
[2]Professor do Centro Universitário Doutor Leão Sampaio/UNILEÃO.

lidar com esses novos fenômenos. A legislação atual, embora busque regular diversos aspectos da internet e da segurança cibernética, ainda apresenta lacunas significativas no que tange à utilização de IA em atividades criminosas. A pesquisa busca, portanto, explorar essas lacunas, discutir as dificuldades impostas pela legislação vigente e propor diretrizes para uma regulação penal mais eficaz e adaptada à realidade digital (Vianna, 2003; Farias et al., 2022).

A falta de uma regulação específica e moderna sobre a utilização de IA em crimes cibernéticos tem gerado um vazio jurídico em várias áreas. As tecnologias baseadas em IA, como algoritmos de aprendizado de máquina e sistemas autônomos, estão se tornando cada vez mais sofisticadas e capazes de realizar atividades prejudiciais de forma mais precisa e discreta. Com isso, surgem questões relativas à responsabilidade legal de ações cometidas por sistemas automatizados e à dificuldade em estabelecer a culpabilidade de indivíduos ou entidades envolvidos no uso indevido dessas tecnologias. Embora existam algumas leis como a Lei 12.737/2012, que tipifica crimes cibernéticos, ou a Lei Geral de Proteção de Dados (LGPD), que regula a proteção de dados pessoais, as normas existentes ainda não cobrem de forma eficiente o uso da IA em atividades criminosas (Pimentel, 2000; Teixeira, 2019).

Outro ponto crítico é a complexidade das tecnologias envolvidas, que tornam difícil a aplicação do direito penal tradicional. As ferramentas de IA têm a capacidade de evoluir, aprender com os dados e modificar seu comportamento, o que levanta questões sobre como essas tecnologias devem ser tratadas do ponto de vista da responsabilidade penal. A dificuldade em rastrear a origem e o controle de sistemas autônomos, como bots de IA ou algoritmos utilizados em fraudes digitais, gera um cenário jurídico desafiador para a aplicação da justiça. A falta de um marco legal claro que trate especificamente desses crimes tem levado a um enfraquecimento na eficácia da resposta judicial frente a crimes cibernéticos assistidos por IA (Pimentel, 2000; Tepedino & Da Guia Silva, 2019).

A pesquisa propõe-se a analisar essas questões jurídicas, enfocando as lacunas existentes na legislação brasileira e os desafios de adequar o direito penal às especificidades dos crimes cibernéticos cometidos por meio da inteligência artificial. A partir de uma revisão bibliográfica, serão examinadas as contribuições de estudiosos e especialistas na área do direito cibernético, com destaque para as obras de Vianna (2003) e Farias et al. (2022), que discutem as implicações da IA no campo jurídico e os riscos que ela impõe à segurança digital. Além disso, serão analisadas propostas legislativas, doutrinárias e jurisprudenciais que buscam tratar da responsabilidade penal em casos envolvendo IA e crimes cibernéticos.

Outro objetivo da pesquisa é explorar as possibilidades de atualização ou criação de novas normativas que abordem especificamente a questão da IA nos crimes cibernéticos. A

legislação vigente precisa ser reformulada para contemplar as novas formas de criminalidade digital, como o uso de IA em ataques cibernéticos, fraudes financeiras e o roubo de dados sensíveis. A criação de uma regulação penal eficaz deve considerar o impacto da IA sobre a privacidade e a segurança dos dados, além de assegurar que os responsáveis por delitos digitais sejam devidamente identificados e responsabilizados (De Souza & Santos, 2024; Farias et al., 2022).

Desta forma, a pesquisa busca propor diretrizes para uma regulação penal mais robusta, que leve em conta a complexidade das tecnologias envolvidas e a necessidade de proteger os direitos fundamentais dos indivíduos no ambiente digital. Essas diretrizes visam não só preencher as lacunas na legislação atual, mas também garantir que o sistema jurídico brasileiro esteja preparado para lidar com os desafios impostos pela evolução constante da IA. Ao propor soluções para uma regulação penal eficaz, a pesquisa contribui para o aprimoramento das políticas públicas de combate aos crimes cibernéticos e para a criação de um ambiente digital mais seguro e justo para todos (Teixeira, 2019; Vidal, 2023).

2 DESENVOLVIMENTO

2.1 METODOLOGIA

A metodologia adotada para este Trabalho de Conclusão de Curso (TCC) foi uma revisão bibliográfica, com o objetivo de analisar os desafios jurídicos e regulatórios da inteligência artificial (IA) no contexto dos crimes cibernéticos. A escolha por uma revisão bibliográfica deve-se ao fato de que esse tipo de pesquisa permite uma análise crítica e detalhada das obras e estudos já publicados sobre o tema, possibilitando uma compreensão ampla das lacunas presentes na legislação brasileira e das soluções propostas para a regulação penal eficaz. A revisão foi realizada com base em artigos acadêmicos, livros, dissertações, teses e legislações nacionais relacionadas ao uso da IA em crimes cibernéticos, priorizando os textos que discutem a adaptação da legislação brasileira às novas tecnologias, especialmente nas esferas do Direito Penal e da proteção de dados digitais.

A pesquisa foi conduzida a partir da coleta de dados secundários, ou seja, dados já disponíveis na literatura especializada. Para garantir a precisão e a relevância das informações coletadas, foi estabelecida uma criteriosa seleção das fontes bibliográficas. Foram priorizadas obras acadêmicas que abordassem tanto os aspectos técnicos da inteligência artificial quanto as implicações jurídicas de sua utilização em crimes cibernéticos. A análise foi focada em publicações que tratam da tipificação de crimes digitais, da proteção de dados pessoais, e da legislação vigente no Brasil, com destaque para a Lei 12.737/2012, conhecida como "Lei

Carolina Dieckmann", que trata de crimes informáticos, e a Lei 9.983/2000, que regulamenta o uso indevido da internet. Além disso, outras fontes relacionadas à interação entre o Direito Penal e a tecnologia digital também foram consideradas, a fim de proporcionar uma visão holística do tema.

O processo de revisão bibliográfica seguiu um percurso cronológico, começando pela análise das obras mais antigas, que lançaram as primeiras discussões sobre o tema, até os estudos mais recentes, que abordaram as novas tendências e soluções para a regulação de crimes digitais. A escolha das fontes foi pautada pela relevância, atualidade e autoridade dos autores, garantindo que os dados obtidos fossem de alta qualidade. As publicações foram analisadas de forma qualitativa, com o objetivo de identificar as principais falhas no sistema jurídico brasileiro frente ao uso da inteligência artificial para a prática de crimes cibernéticos e as estratégias em desenvolvimento para superar esses desafios.

Na condução da pesquisa, foi fundamental observar as dificuldades enfrentadas pela legislação atual em lidar com os crimes cibernéticos assistidos por IA, como a complexidade da tipificação penal desses delitos e a dificuldade de atribuição de responsabilidade a sistemas autônomos. A metodologia envolveu também a identificação das falhas nas regulamentações existentes, especialmente em relação à ausência de normas específicas sobre o uso da inteligência artificial no contexto digital. O enfoque foi dado às implicações dessas lacunas para a eficácia da justiça penal, considerando a evolução constante das tecnologias e suas aplicações no âmbito dos crimes cibernéticos.

A revisão bibliográfica permitiu a proposição de diretrizes para uma regulação penal mais eficaz, com a atualização das normas vigentes e a criação de novas regulamentações que levassem em consideração os desafios contemporâneos dos crimes digitais. A metodologia adotada proporcionou uma abordagem abrangente e crítica do tema, com base em fontes especializadas e atualizadas, oferecendo subsídios para a melhoria da regulação penal no Brasil. Ao utilizar uma metodologia rigorosa e bem estruturada, foi possível garantir a validade e a confiabilidade dos resultados obtidos, permitindo que os achados da pesquisa possam ser utilizados para fundamentar futuras discussões acadêmicas e políticas públicas sobre o tema.

2.2 REFERENCIAL TEÓRICO

2.2.1Conceitos e Definições de Inteligência Artificial (IA)

A Inteligência Artificial (IA) é um campo interdisciplinar que envolve o desenvolvimento de sistemas computacionais capazes de realizar tarefas que, normalmente, exigem inteligência humana, como reconhecimento de padrões, tomada de decisões, resolução de problemas complexos e aprendizado. (RUSSELL; NORVIG, 2022)A IA pode ser definida como a simulação de processos de inteligência humana por meio de algoritmos e máquinas, com o objetivo de imitar a cognição humana (COPPIN, 2004). De acordo com Ferreira (2005), a IA envolve sistemas que percebem, raciocinam, aprendem, resolvem problemas e até interagem com o ambiente, sendo um reflexo do comportamento inteligente humano. Nesse sentido, a IA busca replicar habilidades cognitivas, como aprendizado, raciocínio lógico e tomada de decisão, por meio de técnicas computacionais avançadas, tais como redes neurais, algoritmos genéticos e lógica *fuzzy*.

O conceito de Inteligência Artificial tem se transformado ao longo do tempo, à medida que novas tecnologias e metodologias de aprendizado de máquina foram desenvolvidas. A IA pode ser dividida em duas categorias principais: IA fraca e IA forte. A IA fraca refere-se a sistemas que são projetados para executar tarefas específicas, sem a capacidade de adquirir consciência ou raciocínio em nível humano. Exemplos de IA fraca incluem assistentes virtuais, sistemas de recomendação e motores de busca. Já a IA forte, conforme argumenta Vianna (2003), envolve a criação de máquinas com capacidades cognitivas semelhantes às humanas, com o potencial de raciocínio generalizado e tomada de decisões em uma ampla variedade de situações. No entanto, a IA forte ainda é um conceito hipotético e está distante de ser alcançada, sendo objeto de debates acadêmicos e filosóficos sobre as limitações da IA.

Uma das principais características da IA é a sua capacidade de aprendizado, que é um dos componentes centrais do campo. De acordo com Pimentel (2000), o aprendizado de máquina *(machine learning)* é uma subárea da IA que permite que os sistemas melhorem seu desempenho automaticamente com base em dados, sem serem explicitamente programados para isso. O aprendizado de máquina tem sido amplamente utilizado para o desenvolvimento de algoritmos que analisam grandes volumes de dados, identificam padrões e fazem previsões, o que é essencial em muitas aplicações da IA, como em diagnósticos médicos, reconhecimento de voz e sistemas de recomendação. No entanto, essa tecnologia também levanta questões éticas sobre a transparência dos processos de decisão automatizados e o potencial para viés nos algoritmos, um ponto que deve ser abordado nas discussões sobre regulamentação da IA.

A definição de IA também implica uma discussão sobre as suas limitações e desafios, como aponta Gimenes (2024). A IA, por ser baseada em dados históricos, pode refletir

preconceitos ou distorções presentes nesses dados, resultando em decisões automatizadas tendenciosas. Isso se aplica especialmente a sistemas de IA utilizados em áreas como o mercado de trabalho, sistemas de crédito e até no sistema de justiça, onde algoritmos podem perpetuar desigualdades sociais. A falta de transparência nos algoritmos e a dificuldade de auditar as decisões automatizadas são problemas que demandam uma resposta regulatória clara e eficaz.

A regulação da IA no Brasil tem avançado com a criação de leis que buscam garantir a segurança e a ética no uso de tecnologias digitais, como a Lei 12.737/2012, também conhecida como "Lei Carolina Dieckmann", que trata de crimes digitais e inclui a tipificação de atos ilícitos cometidos com o uso de dispositivos informáticos. Segundo Moreira (2024), a legislação brasileira ainda está em processo de adaptação para lidar adequadamente com a crescente utilização da IA em diversas áreas, especialmente no contexto dos crimes cibernéticos. A falta de uma regulação específica para a IA dificulta a identificação clara de responsabilidades, especialmente quando se trata de sistemas autônomos que tomam decisões sem intervenção humana.

2.2.2 Evolução da IA e seu Impacto no Mundo Digital

A Inteligência Artificial (IA) tem evoluído significativamente desde suas primeiras concepções, com o objetivo de criar máquinas capazes de imitar a cognição humana. Inicialmente, os esforços para desenvolver IA estavam focados em sistemas de processamento simbólico, onde as máquinas eram programadas para seguir regras lógicas e algoritmos definidos para resolver problemas. Porém, ao longo das décadas, com o avanço dos algoritmos de aprendizado de máquina e do aumento da capacidade computacional, a IA passou a ser capaz de aprender com os dados e melhorar suas funções de maneira autônoma, conforme observado por Teixeira (2019). Este avanço reflete uma transição importante, onde a IA deixa de ser apenas uma ferramenta predefinida para se tornar uma tecnologia adaptativa e dinâmica, capaz de aprender e se aprimorar.

O impacto da evolução da IA no mundo digital tem sido profundo, especialmente com o desenvolvimento de tecnologias como redes neurais profundas e algoritmos de aprendizado supervisionado e não supervisionado. Como aponta Pimentel (2000), a IA se tornou um motor central em diversas inovações digitais, desde a personalização de conteúdos em plataformas de streaming até o desenvolvimento de assistentes virtuais que interagem de maneira fluida com os usuários. Esses avanços não apenas aumentaram a eficiência e a automação de

processos, mas também criaram novas possibilidades em áreas como medicina, marketing e finanças, transformando a forma como as empresas e os consumidores interagem. Por exemplo, a IA tem sido utilizada para diagnosticar doenças com maior precisão, prever tendências de consumo e otimizar decisões financeiras, entre outras aplicações.

A crescente dependência de IA também tem gerado desafios e preocupações no campo jurídico. A regulação da IA, como argumenta Pinheiro (2013), é um dos principais pontos de debate, especialmente em relação à proteção de dados pessoais e privacidade. A IA, ao processar grandes volumes de dados pessoais, tem o potencial de infringir direitos fundamentais, como a privacidade, que são essencialmente vulneráveis em um ambiente digital. Vidal (2024) discute que a arquitetura digital, ou a forma como as plataformas e tecnologias digitais são desenhadas, desempenha um papel fundamental na regulação do direito à privacidade, sendo necessária uma abordagem que integre a segurança digital e o respeito aos direitos do usuário. O uso de IA em áreas como marketing digital e redes sociais levanta questões sobre como a coleta de dados deve ser realizada de maneira ética e legal, sem comprometer os direitos dos indivíduos.

Além dos aspectos de privacidade, a IA também apresenta desafios no que diz respeito à responsabilidade civil em casos de danos causados por sistemas autônomos. Tepedino e Da Guia Silva (2019) abordam os desafios jurídicos relacionados à responsabilidade de máquinas inteligentes que operam sem supervisão humana direta, como carros autônomos e sistemas de recomendação de decisões financeiras. Em situações onde a IA toma decisões que causam danos, surge a questão sobre quem deve ser responsabilizado: os desenvolvedores da tecnologia, as empresas que a implementam ou as próprias máquinas? Este debate levanta a necessidade de uma regulamentação mais robusta e flexível, que leve em consideração as especificidades da IA e seu impacto na vida cotidiana.

A regulação dos crimes cibernéticos também tem se tornado uma prioridade à medida que a IA é utilizada tanto para combater quanto para perpetrar atividades criminosas. Farias et al. (2022) destacam que a IA tem sido usada para detectar e prevenir crimes cibernéticos, como fraudes digitais e ataques de hackers, mas também pode ser empregada por criminosos para automatizar atividades ilícitas em uma escala nunca antes vista. A combinação de IA com ferramentas de anonimato, como criptomoedas, cria um novo ambiente de risco no qual a legislação precisa se adaptar rapidamente. No Brasil, como observa De Sousa e Santos (2024), o sistema legal ainda enfrenta dificuldades para lidar com as novas formas de crimes digitais, sendo urgente a atualização das leis para abranger a complexidade desses crimes e suas implicações legais.

Outro aspecto crucial do impacto da IA no mundo digital é sua relação com a pornografia infantil e outros conteúdos ilícitos. A utilização de IA para identificar e bloquear conteúdos ilegais tem sido uma ferramenta essencial na luta contra crimes cibernéticos, como aponta Araújo (2023). No entanto, a rápida evolução das tecnologias de IA também tem levado ao surgimento de novos desafios, como a criação de imagens realistas de pornografia infantil geradas por IA. A tipificação dessas imagens e a regulamentação do uso de IA nesse contexto são questões ainda em aberto, que exigem um esforço conjunto entre legisladores, desenvolvedores e órgãos de segurança pública.

A evolução da IA também afeta o mercado de trabalho, com a automação de processos e a criação de novos tipos de empregos. Segundo Lee (2019), a automação promovida pela IA pode reduzir a necessidade de força de trabalho em áreas específicas, enquanto cria demanda por profissionais qualificados em áreas como ciência de dados, aprendizado de máquina e ética da IA. A transformação digital exigirá uma adaptação das habilidades dos trabalhadores, além de mudanças no sistema educacional para formar especialistas em áreas emergentes da IA. Isso pode gerar tanto oportunidades quanto desafios, dependendo da capacidade dos sistemas de educação e das políticas públicas em se ajustarem às novas exigências do mercado.

O impacto da IA no mundo digital reflete um processo de transformação contínua e acelerada, com implicações significativas tanto para o campo jurídico quanto para a sociedade em geral. A evolução tecnológica exige que a legislação acompanhe de forma proativa as inovações, garantindo que a IA seja utilizada de maneira ética e responsável. Pimentel (2000) e Vianna (2003) afirmam que, além da regulação jurídica, é essencial promover uma discussão pública sobre os limites da IA e seus efeitos sobre a autonomia individual e a segurança coletiva, para que sua implementação seja benéfica para todos os envolvidos.

2.2.3 Definição e Classificação dos Crimes Cibernéticos

Os crimes cibernéticos, também conhecidos como delitos digitais, envolvem atividades ilícitas realizadas por meio de computadores ou dispositivos conectados à internet. De acordo com Vianna (2003), os crimes cibernéticos abrangem uma ampla gama de condutas ilegais, que vão desde fraudes digitais e roubo de dados até ataques cibernéticos a sistemas críticos e a disseminação de conteúdo ilícito. A crescente digitalização das atividades cotidianas e o uso generalizado da internet têm facilitado a ocorrência desses crimes, trazendo

à tona novas questões legais e desafios para os sistemas jurídicos, que ainda estão em processo de adaptação às realidades do mundo digital.

A classificação dos crimes cibernéticos pode ser feita de diversas maneiras, mas uma das abordagens mais comuns é a categorização com base no tipo de conduta realizada. Pimentel (2000) sugere uma divisão entre crimes cibernéticos primários, que envolvem diretamente o uso de tecnologia para cometer delitos, e crimes cibernéticos secundários, que consistem em atividades ilícitas tradicionais (como fraudes, roubo ou extorsão), mas cometidas utilizando a tecnologia. Os crimes primários incluem, por exemplo, o hacking, a distribuição de malware, e o ataque a sistemas de computadores, enquanto os crimes secundários envolvem, por exemplo, fraudes bancárias ou o roubo de identidade realizadas por meio da internet.

A Lei 12.737/2012, conhecida como "Lei Carolina Dieckmann", foi um marco importante na legislação brasileira sobre crimes cibernéticos. Ela tipificou crimes relacionados a dispositivos informáticos, como a invasão de dispositivos, o acesso não autorizado a sistemas de computadores, a alteração de dados e a divulgação de informações sem consentimento. A norma também se aplica a casos em que a vítima sofre prejuízos materiais ou reputacionais devido a esses crimes, estabelecendo penalidades que variam de detenção a reclusão, dependendo da gravidade do ato cometido. A criação dessa lei foi um passo importante para enfrentar as novas formas de criminalidade emergentes no ambiente digital.(BRASIL,2010)

Outro importante marco legislativo no Brasil é a Lei 9.983/2000, que trata de crimes digitais e o uso indevido da internet. Embora sua aplicação seja mais ampla, essa legislação também abrange delitos como a disseminação de conteúdo obsceno e a utilização indevida de dados pessoais na rede, proporcionando um arcabouço jurídico mais robusto para lidar com crimes relacionados à internet. O texto da Lei 9.983/2000 foi posteriormente complementado e ajustado para se adequar às novas ameaças cibernéticas, com a introdução de penalidades mais rigorosas e a previsão de medidas preventivas, como a remoção de conteúdos prejudiciais.

A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) também desempenha um papel relevante na tipificação de crimes cibernéticos relacionados à privacidade e ao uso indevido de dados. Farias et al. (2022) destacam que essa lei foi criada para regular o tratamento de dados pessoais, estabelecendo normas para a coleta, armazenamento e compartilhamento dessas informações. Entre os crimes que podem ocorrer no contexto da

LGPD estão o vazamento de dados, o uso não autorizado de informações pessoais, e a invasão de privacidade, que são penalizados severamente, com multas e outras sanções.

A classificação dos crimes cibernéticos também pode ser feita com base na intenção do criminoso. Quando o objetivo é causar danos ao sistema ou roubar informações, temos crimes como o hacking, o malware e os ataques DDoS (*Distributed Denial of Service),* que têm como foco o comprometimento de sistemas e dados. Vianna (2003) observa que esses ataques podem ter efeitos devastadores em empresas e governos, podendo afetar a segurança nacional e a estabilidade econômica. Por outro lado, há crimes cibernéticos voltados à exploração financeira, como as fraudes bancárias e o roubo de identidade, que têm como alvo os recursos financeiros das vítimas.

Outro tipo relevante de crime cibernético é o relacionado à propriedade intelectual. A pirataria digital, como o download não autorizado de conteúdo protegido por direitos autorais, é uma das formas mais comuns desse tipo de delito. A legislação brasileira, por meio da Lei 9.610/1998, que rege os direitos autorais, tipifica como crime a reprodução não autorizada de obras protegidas, seja por meio de cópias digitais, seja pela distribuição de conteúdo sem a devida permissão dos detentores dos direitos. Essa questão é especialmente relevante no contexto digital, onde a disseminação de conteúdos ocorre com grande rapidez e em grande escala.(BRASIL, 1998).

Além dos crimes de propriedade intelectual e fraudes, a internet também tem sido usada para a propagação de discursos de ódio, pornografia infantil e outros conteúdos prejudiciais. A Lei 13.718/2018, que criminaliza a divulgação de imagens íntimas sem consentimento, e a Lei 12.737/2012, mencionada anteriormente, são legislações essenciais para combater esses crimes(BRASIL, 2018; BRASIL, 2012). O uso da internet para difundir pornografia infantil, por exemplo, é um crime previsto pelo artigo 241-A do Estatuto da Criança e do Adolescente – ECA (BRASIL, 1990), com penas severas para os infratores. A legislação também trata do combate à pedofilia digital, com ações que buscam a remoção de conteúdos e a punição dos responsáveis pela criação e distribuição de imagens.

Ademais, no contexto dos crimes cibernéticos, o fenômeno da responsabilidade penal de empresas também se destaca. Empresas podem ser responsabilizadas por falhas na segurança de seus sistemas, como no caso de vazamentos de dados que afetam a privacidade dos usuários. A legislação brasileira, incluindo o Código Penal e a Lei 12.965/2014, conhecida como o Marco Civil da Internet, estabelece responsabilidades tanto para os usuários da internet quanto para os provedores de serviços digitais, como plataformas de redes sociais e empresas de hospedagem de dados(BRASIL, 2014). Esses regulamentos visam

garantir que as empresas adotem medidas adequadas para proteger os dados pessoais e evitar o envolvimento em práticas criminosas.

2.2.4 Relação entre IA e Crimes Cibernéticos

A relação entre Inteligência Artificial (IA) e crimes cibernéticos tem se intensificado à medida que a tecnologia avança e o ambiente digital se torna cada vez mais complexo. A IA, por sua natureza, oferece ferramentas poderosas tanto para a prevenção quanto para a perpetrção de delitos cibernéticos. Por um lado, sistemas baseados em IA têm sido empregados para detectar padrões de comportamento suspeitos e identificar ameaças em tempo real, sendo fundamentais para combater ataques de *phishing,* fraudes digitais e outras atividades criminosas na internet (Farias et al., 2022). Porém, por outro lado, criminosos também têm utilizado essas mesmas tecnologias para potencializar seus ataques, criando sistemas autônomos capazes de realizar ações prejudiciais de forma mais eficiente e dissimulada, como no caso de ataques DDoS *(Distributed Denial of Service)* baseados em IA.

A utilização de IA por cibercriminosos é uma preocupação crescente no campo da segurança cibernética. De acordo com Vianna (2003), ferramentas de IA são empregadas para desenvolver *malwares* que são capazes de se adaptar e modificar seu comportamento de acordo com os sistemas que tentam infectar, tornando-se mais difíceis de detectar pelos mecanismos tradicionais de segurança. Além disso, a IA tem sido usada para criar ataques sofisticados de engenharia social, como os já conhecidos golpes de *phishing,* onde os sistemas de IA analisam grandes volumes de dados para personalizar e tornar os ataques mais convincentes, aumentando as chances de sucesso. Essas práticas exigem uma adaptação constante dos profissionais de segurança e das legislações para mitigar os riscos que acompanham o avanço da tecnologia.

Por outro lado, a IA também tem um papel central na prevenção de crimes cibernéticos, especialmente no que se refere à proteção de dados sensíveis e à identificação de atividades fraudulentas. Ferramentas de IA, como algoritmos de aprendizado de máquina, são amplamente utilizadas para monitorar transações financeiras em tempo real, identificar padrões anômalos e prevenir fraudes em setores como o bancário e o *e-commerce* (Farias et al., 2022). Além disso, tecnologias de IA também são aplicadas na detecção de vulnerabilidades em sistemas de redes e servidores, o que permite que as empresas tomem medidas preventivas antes que ocorram invasões ou outros tipos de ataques. Isso tem

contribuído para um ambiente digital mais seguro, minimizando os danos causados por crimes cibernéticos e melhorando a resposta a incidentes de segurança.

No campo jurídico, a combinação de IA com crimes cibernéticos tem gerado um novo conjunto de desafios para a legislação, uma vez que as leis precisam acompanhar a evolução das tecnologias de forma eficaz. A utilização de IA em crimes digitais, como o uso de algoritmos para manipulação de dados e a criação de *deepfakes* (imagens ou vídeos falsificados com alta credibilidade), exige que os sistemas legais, como o Código Penal e leis específicas de proteção de dados, sejam atualizados constantemente (Teixeira, 2019). A criação de normas específicas sobre a responsabilidade da IA em casos de crimes cibernéticos e a definição de mecanismos para responsabilizar tanto os desenvolvedores dessas tecnologias quanto os criminosos que as utilizam ainda são questões em debate, conforme discutido por autores como Farias et al. (2022) e Pimentel (2000).

A relação entre IA e crimes cibernéticos também demanda uma atenção maior para a ética no uso dessas tecnologias. A crescente automação de atividades no ciberespaço tem levantado questões sobre a responsabilidade dos sistemas de IA em ações que podem causar danos significativos. Tepedino e Da Guia Silva (2019) afirmam que a atribuição de responsabilidade civil em casos envolvendo IA e crimes cibernéticos é um tema emergente, pois muitas vezes o sistema de IA opera de forma autônoma, tornando difícil identificar um responsável direto pelos danos causados. O desenvolvimento de uma regulamentação que defina claramente as responsabilidades jurídicas em relação ao uso de IA para a prevenção e a realização de crimes digitais será fundamental para garantir a proteção dos usuários e a integridade do ambiente digital.

2.3 RESULTADOS E DISCUSSÃO

2.3.1 O Uso da Inteligência Artificial para a Prática de Crimes Cibernéticos

A aplicação da inteligência artificial (IA) para fins ilícitos, em especial no contexto dos crimes cibernéticos, tem se intensificado com o avanço tecnológico, tornando-se uma das maiores ameaças contemporâneas à segurança digital. O uso malicioso da IA amplia as possibilidades de ataque, não apenas em termos quantitativos, mas sobretudo qualitativos, uma vez que permite a realização de condutas altamente sofisticadas, de difícil rastreabilidade e de grande impacto social. Tais práticas desafiam os atuais modelos de tipificação penal e

exigem novas estratégias de regulação e responsabilização. A capacidade da IA de aprender com dados massivos e de se adaptar a novos contextos torna-a uma ferramenta poderosa tanto para o bem quanto para a prática do mal (PIMENTEL, 2000).

Um dos exemplos mais emblemáticos do uso da IA para fins criminosos é a produção de *deepfakes* – vídeos, áudios ou imagens manipuladas digitalmente para simular pessoas reais em situações comprometedoras ou enganosas. Essas falsificações, baseadas em redes neurais generativas, têm gerado sérias implicações legais e éticas, pois atingem diretamente direitos fundamentais como a imagem, a honra e a privacidade. No Brasil, apesar da Constituição proteger esses direitos, ainda não há legislação penal específica que tipifique o uso de *deepfakes* com fins ilícitos, o que gera um vácuo jurídico considerável (PIMENTEL, 2000). A ausência de previsões legais claras dificulta a responsabilização dos autores e alimenta a impunidade.

A tipificação penal de condutas envolvendo *deepfakes* esbarra em uma série de desafios jurídicos. Conforme observa Marcacini (2002), a legislação penal tradicional foi pensada a partir de um paradigma humanista, centrado em ações humanas conscientes e voluntárias. Quando se trata de crimes praticados com o auxílio de tecnologias autônomas e autorreguladas, como ocorre nas manipulações por IA, torna-se necessário repensar categorias como dolo, culpa, autoria e participação. O direito penal ainda não está preparado para enfrentar crimes cuja execução é mediada por sistemas artificiais que operam de forma independente ou semi-autônoma.

Outro campo sensível à atuação criminosa da IA diz respeito às fraudes financeiras e ao *phishing* automatizado. Com o uso de sistemas baseados em aprendizado de máquina, criminosos conseguem identificar padrões de comportamento de consumidores, simular páginas bancárias com precisão, enviar e-mails personalizados e realizar ataques massivos de engenharia social com altíssima taxa de sucesso (CARNEIRO, 2012). Conforme aponta Gimenes (2024), essas práticas aumentam a complexidade da investigação, pois os ataques são descentralizados, realizados em larga escala e continuamente aperfeiçoados pelos próprios algoritmos.

A Lei 11.419/2006, que trata da informatização do processo judicial, não contempla as especificidades do cibercrime automatizado, deixando lacunas quanto à coleta de provas e à responsabilização dos agentes em contextos mediados por inteligência artificial. Essa limitação legislativa contribui para a ineficiência da persecução penal, comprometendo a resposta estatal frente aos crimes praticados com IA. Além disso, os recursos tecnológicos que permitiriam a detecção e rastreio das fraudes nem sempre estão disponíveis aos órgãos de

segurança pública, aprofundando a assimetria entre agentes criminosos e as instituições responsáveis pela repressão (BRASIL, 2006).

A IA também tem sido amplamente utilizada para o desenvolvimento de *malwares, ransomwares e botnets* inteligentes, que conseguem invadir sistemas, sequestrar dados e extorquir valores com alta taxa de sucesso. Esses ataques, muitas vezes, se baseiam em algoritmos que estudam as vulnerabilidades de redes, adaptam-se em tempo real e se escondem de mecanismos de defesa tradicionais (PIMENTEL, 2000). O desafio, segundo Vianna (2003), é que as ferramentas de ciberdefesa ainda não acompanham a sofisticação dos novos *malwares*, tornando as respostas legais e técnicas desatualizadas diante da crescente complexidade dos ataques.

As implicações legais desses ataques vão desde a necessidade de revisão das leis penais até a reformulação das estratégias de cooperação internacional. A inexistência de tratados específicos que contemplem o uso da IA em cibercrimes compromete a atuação integrada entre países. Além disso, os dispositivos legais existentes, como a Lei 12.737/2012, focam principalmente na invasão de dispositivos informáticos por meios convencionais, sem abarcar o uso de tecnologias baseadas em inteligência artificial, deixando brechas que impedem a responsabilização efetiva.

Com a automação do cibercrime, o cenário torna-se ainda mais preocupante. Sistemas baseados em IA já são capazes de realizar ataques de forma autônoma, sem supervisão direta de um operador humano. Isso tem transformado o perfil do criminoso digital, que deixa de ser um especialista técnico para tornar-se um agente que apenas programa a IA e a deixa operar (LOSANO, 1974). Esse novo paradigma impõe um duplo desafio: por um lado, à doutrina penal, que deve repensar os conceitos tradicionais de imputabilidade; por outro, à técnica legislativa, que precisa criar normas suficientemente abertas para abarcar a dinâmica das tecnologias emergentes.

A automação também permite que crimes cibernéticos sejam cometidos em escala global e em tempo real, com impactos diretos sobre instituições bancárias, hospitais, redes de energia e outras infraestruturas críticas. Segundo Pinheiro (2013), os ataques não são apenas mais numerosos, mas também mais eficazes, pois utilizam a própria infraestrutura digital como meio e alvo, explorando brechas técnicas e jurídicas. A legislação nacional, com sua vocação territorial e estática, não consegue acompanhar a fluidez dos ataques e tampouco delimitar jurisdições de forma clara, o que compromete a eficácia da resposta penal.

Outro problema identificado é a dificuldade em definir a linha entre o uso lícito e o uso criminoso da IA. Muitos dos algoritmos utilizados em cibercrimes são, na verdade,

ferramentas legítimas que foram desviadas de sua função original. Essa ambiguidade entre o uso ético e o uso ilícito torna o controle legislativo mais delicado, exigindo maior precisão normativa para evitar que se criminalize condutas tecnológicas legítimas ou, inversamente, se deixem impunes práticas claramente abusivas e danosas à sociedade.

O uso de IA também desafia os métodos tradicionais de investigação criminal. Os *logs* de dados, endereços IP e outras evidências digitais podem ser manipulados ou mascarados por sistemas de IA, dificultando a coleta e validação da prova. Além disso, algoritmos utilizados em *deep learning* muitas vezes operam como "caixas-pretas", tornando inviável a rastreabilidade e a explicação dos seus processos decisórios. Essa opacidade compromete tanto a responsabilização penal quanto a defesa do acusado, gerando insegurança jurídica e comprometendo o devido processo legal (FERREIRA, 2005).

A possibilidade de utilização da IA em ataques contra crianças e adolescentes também tem crescido, especialmente com a produção e disseminação de conteúdo pornográfico infantil por meio de imagens hiper-realistas. Conforme alerta Araújo (2023), a IA já é capaz de criar conteúdos inteiramente fictícios que simulam menores de idade, sem envolver vítimas reais, mas com potencial ofensivo equivalente. A ausência de legislação específica para essas imagens realistas compromete os esforços de repressão e requer urgentes modificações legais no ECA e no Código Penal.

Nesse sentido, a regulação do uso da IA nos crimes cibernéticos precisa ir além da simples atualização normativa. É necessário construir uma abordagem sistemática que envolva cooperação internacional, capacitação técnica das autoridades, investimento em tecnologia e educação digital da população. A ausência de uma política pública coerente e integrada sobre cibersegurança deixa o Brasil vulnerável, não apenas como nação, mas também como parte do ecossistema global da informação.

2.2.2 Desafios Jurídicos na Regulamentação dos Crimes Cibernéticos Envolvendo IA

A crescente utilização da inteligência artificial (IA) em crimes cibernéticos revela profundas fragilidades na estrutura legislativa brasileira, que ainda não está preparada para lidar com as especificidades dessa nova realidade tecnológica. As normas penais atualmente em vigor foram elaboradas com base em pressupostos clássicos de ação humana consciente, o que dificulta sua aplicação em casos em que sistemas de IA são utilizados como ferramentas ou atuam com certo grau de autonomia. Nesse cenário, torna-se urgente o desenvolvimento de uma legislação mais robusta, que considere a complexidade das infrações digitais

contemporâneas, como apontam Moreira (2024) e a própria lacuna existente desde a Lei nº 9.609/1998, voltada à proteção da propriedade intelectual de softwares, mas insuficiente para crimes cibernéticos modernos.

Essa fragilidade legislativa é ainda mais evidente quando analisamos a ausência de uma regulação penal eficaz voltada especificamente para os crimes cibernéticos praticados com auxílio de IA. Gimenes (2024) destaca que, embora o Brasil tenha avançado com a Lei Carolina Dieckmann (Lei nº 12.737/2012), essa norma ainda se mostra genérica e limitada, pois não contempla, por exemplo, o uso de algoritmos para fraudes, extorsões, invasões automatizadas e ataques distribuídos via redes neurais artificiais. A normatividade atual é incapaz de acompanhar a velocidade com que os cibercriminosos adaptam e utilizam novas tecnologias, especialmente aquelas que escapam da previsibilidade dos sistemas judiciais.

Um dos debates mais relevantes no campo jurídico é a distinção entre o uso da IA como mera ferramenta e sua atuação como agente autônomo. A responsabilização penal pressupõe a existência de dolo ou culpa, atributos tradicionalmente vinculados à consciência humana. Contudo, quando um sistema de IA executa um crime sem interferência direta ou previsível do programador, surgem questionamentos sobre quem deve ser responsabilizado: o criador do algoritmo, o usuário, o operador ou ninguém? Marcacini (2002) alerta que o direito penal precisa urgentemente desenvolver teorias capazes de absorver essa nova forma de intervenção técnica, sob pena de se tornar obsoleto frente à transformação digital.

Pimentel (2000) corrobora essa preocupação ao afirmar que os sistemas de IA podem operar de forma autônoma com base em aprendizado de máquina, criando situações onde não há vínculo direto entre o criador e o comportamento final do programa. A ausência de controle direto sobre os resultados das decisões algorítmicas complica a atribuição de responsabilidade penal, pois o nexo causal entre conduta e resultado passa a ser mediado por uma “caixa-preta” técnica. Tal opacidade algorítmica dificulta o enquadramento penal tradicional e exige novos critérios jurídicos que considerem a previsibilidade, a intencionalidade e o risco sistêmico da tecnologia utilizada.

Além das dificuldades teóricas, a prática penal enfrenta obstáculos concretos na identificação e punição dos crimes digitais mediados por IA. A coleta de provas digitais depende da integridade dos dados, da cooperação de provedores e da rastreabilidade das ações, o que se torna extremamente complicado diante da atuação de sistemas autônomos, que muitas vezes operam fora de jurisdição nacional. Pinheiro (2013) destaca que a capacidade da IA de ocultar rastros, modificar dados em tempo real e agir em ambientes criptografados

compromete a eficácia investigativa e exige um novo modelo probatório baseado em auditoria de algoritmos e perícia técnica especializada.

Paralelamente, surgem questões sensíveis envolvendo a proteção da privacidade e a regulação de dados pessoais. Como lembra Vidal (2024), a própria arquitetura da internet e das plataformas digitais facilita a coleta massiva de dados, muitas vezes sem o consentimento adequado dos usuários. A IA, ao operar com base em grandes volumes de dados (big data), frequentemente viola a privacidade sob o pretexto da personalização de serviços ou da automação de tarefas. Quando utilizada para fins criminosos, essa prática agrava ainda mais o cenário de vulnerabilidade dos cidadãos, exigindo marcos legais que protejam a integridade dos dados e estabeleçam limites para seu uso por algoritmos.

No contexto dos crimes cibernéticos, o respeito aos direitos fundamentais no ambiente digital assume uma centralidade inegável. Guerra (2012) afirma que a cidadania digital deve ser reconhecida como uma extensão dos direitos humanos clássicos, incluindo a proteção à dignidade, à privacidade, à informação e à segurança. O ambiente virtual, por sua própria natureza, exige do Estado uma atuação proativa na construção de mecanismos jurídicos que assegurem a efetividade desses direitos diante de ameaças invisíveis, muitas vezes automatizadas e altamente sofisticadas.

Um instrumento internacional essencial no combate aos crimes cibernéticos é a Convenção de Budapeste sobre o Cibercrime, que estabelece parâmetros para a definição de crimes informáticos, coleta de provas digitais e cooperação internacional entre autoridades judiciais. O Brasil formalizou sua adesão a esse tratado por meio do Decreto nº 11.491, de 18 de abril de 2023, promulgando integralmente a convenção e incorporando-a ao ordenamento jurídico nacional. Essa medida, conforme Barone (2024), representa um avanço indispensável diante da crescente sofisticação dos crimes digitais, sobretudo aqueles potencializados por inteligência artificial.

Outro desafio que merece destaque é o risco de violação de garantias constitucionais na tentativa de regular a IA de forma apressada e pouco técnica. O princípio da legalidade penal, que exige tipificações claras e prévias, pode ser comprometido se a legislação for construída com conceitos vagos ou excessivamente abertos, como “comportamento algorítmico indevido” ou “autonomia criminosa”. Uma regulação penal eficaz deve equilibrar a precisão normativa com a flexibilidade necessária para abarcar inovações tecnológicas, sem comprometer as garantias individuais previstas no ordenamento jurídico.

A complexidade técnica da IA impõe, também, um desafio à formação dos operadores do direito. Juízes, promotores e advogados precisam compreender minimamente o

funcionamento dos algoritmos e suas implicações práticas para poder julgar com justiça e segurança. A ignorância técnica pode levar a decisões equivocadas, tanto pela criminalização de condutas legítimas quanto pela impunidade de crimes sofisticados. Nesse sentido, é urgente incluir o estudo da IA e da informática jurídica nos currículos dos cursos de Direito, como defendem diversos autores contemporâneos, entre eles Losano (1974).

É importante observar que os crimes cibernéticos com IA muitas vezes envolvem múltiplas jurisdições, o que torna a atuação estatal ainda mais desafiadora. Sistemas de IA podem operar em servidores localizados fora do país, sendo controlados por indivíduos também fora do alcance da legislação nacional. Assim, o desafio não é apenas normativo, mas também logístico e diplomático, demandando cooperação jurídica internacional mais eficiente e ágil, baseada em tratados e acordos de assistência mútua.

Outro aspecto crucial é a definição de limites éticos para o uso da IA. Mesmo em casos em que a tecnologia é utilizada para fins lícitos, como na coleta de informações ou no monitoramento de redes, é preciso garantir que seu emprego respeite os direitos fundamentais e o devido processo legal. A linha entre segurança e vigilância é tênue, e uma legislação penal que utilize a IA de maneira indiscriminada pode se transformar em um instrumento de abuso estatal, conforme alertado por Vidal (2024) ao tratar da arquitetura da internet como meio de controle.

A regulamentação da IA em crimes cibernéticos também precisa lidar com a rápida obsolescência das tecnologias. Leis que hoje parecem eficazes podem se tornar inúteis em poucos anos, diante da velocidade com que surgem novos métodos e ferramentas digitais. Por isso, é necessário adotar um modelo regulatório que combine normas rígidas com princípios orientadores de interpretação, permitindo que o Judiciário acompanhe as transformações sem a necessidade constante de reformas legislativas.

Em suma, os desafios jurídicos impostos pela inteligência artificial no contexto dos crimes cibernéticos revelam a necessidade de um novo paradigma normativo, técnico e institucional. A estrutura legal tradicional, baseada em ações humanas previsíveis, já não é suficiente para dar conta das condutas criminosas mediadas por algoritmos. Superar essas barreiras exige uma abordagem multidisciplinar, que envolva juristas, engenheiros, especialistas em segurança digital e formuladores de políticas públicas.

Portanto, o enfrentamento jurídico dos crimes cibernéticos envolvendo IA deve ser feito com prudência, conhecimento técnico e respeito aos direitos fundamentais. Apenas assim será possível criar um ambiente digital seguro, equilibrado e justo, no qual as inovações tecnológicas estejam a serviço da sociedade e não da criminalidade

2.3.3 Estratégias e Soluções para o Enfrentamento dos Crimes Cibernéticos Envolvendo IA

Diante da complexidade crescente dos crimes cibernéticos potencializados pela inteligência artificial (IA), torna-se indispensável a formulação de estratégias integradas e inovadoras para enfrentamento desse fenômeno. O primeiro passo nesse processo é o fortalecimento da legislação nacional, que deve ser atualizada para contemplar as novas modalidades de condutas ilícitas associadas à IA. Conforme Moreira (2024), é urgente uma normatização específica que tipifique, de forma clara, as práticas criminosas mediadas por IA, como a criação de deepfakes, automação de ataques, e uso de algoritmos para fraudes e manipulações digitais. A ausência de normas objetivas compromete a previsibilidade jurídica e favorece a impunidade.

No âmbito interno, destaca-se a tramitação do Projeto de Lei nº 2.338, de 2023, que propõe instituir o Marco Legal da Inteligência Artificial no Brasil. A proposta tem por objetivo estabelecer princípios, direitos e deveres para o uso ético, seguro e responsável da inteligência artificial no país, criando também parâmetros para a responsabilização em casos de uso indevido da tecnologia. O PL 2.338/2023 dialoga diretamente com a Estratégia Nacional de Cibersegurança (Decreto nº 11.141/2022) e com a Convenção de Budapeste, compondo um arcabouço jurídico e estratégico para fortalecer a segurança digital e proteger os direitos fundamentais dos cidadãos no ambiente virtual.

Outro aspecto fundamental para o enfrentamento eficaz desses crimes é o investimento em capacitação técnica dos operadores do direito. Juízes, promotores, delegados e advogados devem compreender minimamente o funcionamento dos sistemas de IA, a lógica algorítmica e os impactos jurídicos das decisões automatizadas. Pinheiro (2013) destaca que a formação multidisciplinar é indispensável para evitar erros na análise de provas digitais, interpretação de condutas e julgamento de casos envolvendo tecnologias emergentes. Essa capacitação também deve se estender às polícias civis e federais, que carecem de pessoal especializado e recursos técnicos adequados para conduzir investigações cibernéticas sofisticadas.

A criação de delegacias especializadas em cibercrimes e unidades forenses digitais é uma das soluções mais eficazes para combater a criminalidade digital com base em IA. Essas unidades devem ser dotadas de equipamentos avançados, acesso a softwares de rastreamento algorítmico e convênios com empresas privadas de tecnologia, que frequentemente detêm informações cruciais sobre os sistemas e plataformas utilizados nas práticas ilícitas. Gimenes

(2024) ressalta que a resposta estatal precisa ser proporcional ao nível de sofisticação dos crimes, o que exige atuação coordenada entre os setores público e privado.

Além da repressão penal, é necessário desenvolver políticas públicas de prevenção e educação digital. Conforme Guerra (2012), a cidadania digital deve ser promovida desde o ensino básico, com conteúdos sobre segurança na internet, reconhecimento de fraudes virtuais e uso consciente da tecnologia. Uma população digitalmente educada é menos vulnerável a golpes de *phishing*, manipulações por IA e disseminação de *fake news*. A educação digital, nesse sentido, funciona como barreira social contra o avanço da criminalidade automatizada, promovendo a inclusão tecnológica aliada à consciência crítica.

Outro caminho promissor é a utilização da própria inteligência artificial como aliada no combate aos crimes digitais. Ferramentas baseadas em IA podem ser empregadas para detectar padrões de comportamento criminoso, monitorar redes suspeitas e antecipar ataques cibernéticos. Farias et al. (2022) apontam que a inteligência artificial, quando usada de forma ética e supervisionada, permite ampliar a capacidade estatal de investigação e resposta, especialmente em contextos de big data e crimes em larga escala. O uso responsável da IA pelo Estado pode compensar, em parte, a desvantagem frente ao avanço dos agentes mal-intencionados.

A regulação do uso da IA também precisa incorporar princípios de transparência e auditoria algorítmica. Conforme Vidal (2024), os algoritmos utilizados em processos sensíveis — seja para investigação, seja para análise probatória — devem ser passíveis de explicação e revisão. A opacidade dos sistemas de IA compromete o controle judicial e pode gerar injustiças, especialmente se decisões forem tomadas com base em códigos inacessíveis às partes envolvidas. Assim, é necessário regulamentar a "explicabilidade" dos algoritmos, garantindo sua auditabilidade tanto em casos de uso lícito quanto ilícito.

A responsabilização penal em crimes envolvendo IA exige a formulação de uma nova dogmática jurídica. Pimentel (2000) argumenta que o direito penal precisa se adaptar à ideia de responsabilidade por risco tecnológico, especialmente quando há uso deliberado de sistemas imprevisíveis ou autônomos. A responsabilização não deve recair apenas sobre o operador final, mas também sobre o programador, o fornecedor da tecnologia e eventuais negligentes na cadeia de uso. Essa abordagem amplia o espectro de responsabilização, respeitando os princípios da legalidade e proporcionalidade.

Outro elemento estratégico é o fortalecimento da cooperação internacional por meio de protocolos multilaterais e parcerias bilaterais. Crimes cibernéticos com IA muitas vezes envolvem agentes distribuídos em diferentes países, o que demanda integração entre polícias,

ministérios públicos e órgãos de inteligência. A participação ativa do Brasil em fóruns internacionais, como a Interpol Digital Crime Center e a OCDE, possibilita o acesso a boas práticas regulatórias, treinamentos especializados e tecnologias de rastreamento de ponta (TEPEDINO; SILVA, 2019). A soberania digital, nesse sentido, só se consolida quando aliada à integração transnacional.

A arquitetura das plataformas digitais também precisa ser regulada para impedir o uso abusivo da IA. Segundo Vidal (2024), muitos crimes ocorrem em ambientes digitais que não impõem limites éticos ou técnicos ao funcionamento de seus algoritmos. Redes sociais, aplicativos de mensagens e *marketplaces* devem ser responsabilizados pela negligência em seus mecanismos de moderação e controle, especialmente quando há omissão deliberada diante de condutas criminosas. A arquitetura digital, nesse sentido, não é neutra, mas influenciadora direta de comportamentos, devendo estar submetida à regulação.

Incentivar a pesquisa acadêmica e o desenvolvimento de tecnologias seguras é outra estratégia crucial. Universidades e centros de pesquisa podem desempenhar papel fundamental no desenvolvimento de soluções tecnológicas que conciliem inovação e segurança. Kuhn (1997) lembra que toda revolução científica implica riscos, mas também oportunidades de reestruturação social. Apoiar pesquisas voltadas à ética da IA, à segurança da informação e ao desenvolvimento de tecnologias *open source* auditáveis é investir em soberania tecnológica e prevenção de crimes.

Desta forma, o combate aos crimes cibernéticos com IA exige um compromisso institucional com a atualização constante. Leis, práticas e tecnologias devem ser revisadas periodicamente à luz das mudanças tecnológicas. Isso requer a criação de comissões permanentes no Legislativo e órgãos técnicos de consulta no Judiciário e Executivo, compostos por especialistas multidisciplinares. Somente com esse esforço contínuo será possível enfrentar os desafios colocados por uma criminalidade que se reinventa com a velocidade da inovação.

3 CONSIDERAÇÕES FINAIS

A presente pesquisa abordou os desafios jurídicos e regulatórios da inteligência artificial (IA) aplicada à prática de crimes cibernéticos, um tema de crescente relevância diante da aceleração tecnológica que marca a era digital. Com a expansão das capacidades da IA, novas formas de criminalidade surgem no ambiente virtual, exigindo do ordenamento jurídico respostas que sejam ao mesmo tempo eficazes, éticas e compatíveis com os direitos

fundamentais. A legislação tradicional, concebida em um contexto de ações humanas diretas e previsíveis, não consegue acompanhar a complexidade das condutas mediadas por sistemas autônomos e algoritmos de aprendizado de máquina, o que compromete a efetividade da justiça penal nesse novo cenário.

O uso da IA em práticas criminosas tem provocado uma ruptura na lógica convencional do Direito Penal, especialmente no que tange à autoria, culpabilidade e responsabilidade. Ferramentas de *deepfake*, *malwares* inteligentes, fraudes automatizadas e ataques cibernéticos com algoritmos adaptativos são apenas alguns exemplos da forma como a tecnologia pode ser utilizada de forma maliciosa. Essas inovações desafiam os mecanismos tradicionais de investigação e punição, pois não apenas dificultam a identificação do agente humano por trás do crime, como também atuam com alto grau de sofisticação e autonomia, reduzindo a eficácia dos métodos forenses tradicionais e da própria legislação vigente.

Além disso, o enfrentamento desses crimes demanda uma reestruturação institucional e normativa profunda. É necessário estabelecer marcos legais que não apenas tipifiquem adequadamente as condutas ilícitas relacionadas à IA, mas que também promovam a responsabilização de agentes indiretos, como desenvolvedores, provedores de tecnologia e plataformas digitais, quando houver falhas ou omissões que facilitem práticas criminosas. Paralelamente, é indispensável garantir que os princípios constitucionais, como legalidade, ampla defesa, contraditório e privacidade, sejam respeitados, mesmo em um contexto altamente tecnificado e volátil como o ciberespaço.

Outra dimensão central do problema é a necessidade de políticas públicas voltadas à prevenção e à educação digital. A sociedade precisa estar preparada para lidar com os riscos da IA, compreendendo tanto seus benefícios quanto os potenciais danos. A atuação estatal deve ir além da repressão e incluir medidas pedagógicas, campanhas de conscientização e programas educacionais que formem cidadãos críticos e conscientes sobre o uso responsável da tecnologia. Da mesma forma, o Estado deve investir em infraestrutura, capacitação de profissionais da justiça e desenvolvimento de ferramentas de monitoramento e análise baseadas na própria inteligência artificial.

A pesquisa também evidenciou a importância da cooperação internacional no combate aos crimes cibernéticos com IA. Dado o caráter transnacional dessas infrações, nenhuma nação será capaz de enfrentá-las de forma isolada. A construção de tratados, acordos bilaterais e mecanismos de assistência jurídica mútua se mostra imprescindível para garantir que criminosos não se beneficiem de lacunas legais e fronteiras digitais. O Brasil, nesse contexto, precisa se alinhar a padrões globais de proteção, investigação e responsabilização, assumindo

uma postura ativa nos debates internacionais sobre ética, segurança e regulação da inteligência artificial.

Portanto, conclui-se que os desafios jurídicos e regulatórios da IA em crimes cibernéticos exigem uma resposta ampla, integrada e dinâmica. Não se trata apenas de atualizar leis, mas de repensar a própria estrutura do sistema de justiça penal à luz das transformações tecnológicas. O futuro da segurança digital e da proteção dos direitos fundamentais dependerá da capacidade dos legisladores, operadores do direito e sociedade em geral de compreenderem os impactos da IA, anteciparem riscos e construírem soluções jurídicas que estejam à altura das inovações que moldam o presente e o futuro da humanidade.

REFERÊNCIAS

ARAÚJO, Adeildo da Silva. *Os desafios no combate à pornografia infantil com o uso da inteligência artificial: um estudo sobre a necessidade de tipificação de imagens realistas no contexto brasileiro*. 2023.

BARONE, Victor. O que é a Convenção de Budapeste. Disponível em: http://www.escrivinhas.blogs.com.br. Acesso em: 14 maio 2025.

BARONE, F. Cooperação internacional e crimes cibernéticos: desafios contemporâneos. *Revista Brasileira de Direito Penal Digital*, v. 3, n. 1, p. 45-67, 2024.

BRASIL. Decreto nº 11.141, de 27 de julho de 2022. Aprova a Estratégia Nacional de Cibersegurança (E-Ciber). *Diário Oficial da União: seção 1*, Brasília, DF, ano 159, n. 142, p. 8, 28 jul. 2022. Disponível em: https://www.in.gov.br/en/web/dou/-/decreto-n-11.141-de-27-de-julho-de-2022-421182201. Acesso em: 1 jul. 2025.

BRASIL. Decreto nº 11.491, de 18 de abril de 2023. Promulga a Convenção sobre o Crime Cibernético, concluída em Budapeste, em 23 de novembro de 2001. *Diário Oficial da União: seção 1*, Brasília, DF, ano 160, n. 74, p. 1, 19 abr. 2023. Disponível em: https://www.in.gov.br/en/web/dou/-/decreto-n-11.491-de-18-de-abril-de-2023-476573791. Acesso em: 1 jul. 2025.

BRASIL. *Estatuto da Criança e do Adolescente (ECA)*. Lei n. 8.069, de 13 de julho de 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 14 maio 2025.

BRASIL. Lei n. 9.609, de 19 de fevereiro de 1998. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9609.htm. Acesso em: 14 maio 2025.

BRASIL. Lei n. 9.983, de 14 de julho de 2000. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L9983.htm. Acesso em: 14 maio 2025.

BRASIL. Lei n. 11.419, de 19 de dezembro de 2006. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11419.htm. Acesso em: 14 maio 2025.

BRASIL. Lei n. 12.737, de 30 de novembro de 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 14 maio 2025.

BRASIL. Projeto de Lei nº 2.338, de 2023. Estabelece princípios, direitos e deveres para o uso da inteligência artificial no Brasil. Disponível em: https://www.camara.leg.br/propostas-legislativas/2378999. Acesso em: 1 jul. 2025.

CARNEIRO, Adeneele Garcia. Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação. *Âmbito Jurídico*, Rio Grande, v. 15, n. 99, abr. 2012. Disponível em: http://www.ambitojuridico.com.br. Acesso em: 14 maio 2025.

COPPIN, Ben. *Inteligência artificial*. Rio de Janeiro: LTC, 2004.

DE SOUSA, Carlos Muryllo Rodrigues; SANTOS, Guilherme Augusto Martins. Crimes cibernéticos e os desafios jurídicos na era digital: análise legislativa, doutrinária e jurisprudencial. *Revista JRG de Estudos Acadêmicos*, v. 7, n. 15, p. e151662-e151662, 2024.

FARIAS, Karina da Hora et al. *Impactos dos crimes cibernéticos e os riscos da inteligência artificial: os pilares do direito na proteção dos dados sensíveis*. 2022.

FERREIRA, Ivette Senise. *Direito & Internet: aspectos jurídicos relevantes*. 2. ed. São Paulo: Quartier Latin, 2005.

GIMENES, Emanuel Alberto Sperandio Garcia. Crimes virtuais. *Revista de Doutrina TRF4*, [s.l.], [s.n.], [s.d.]. Disponível em: http://www.revistadoutrina.trf4.jus.br. Acesso em: 14 maio 2025.

GUERRA, Sidney. *Direitos humanos & cidadania*. São Paulo: Atlas, 2012.

KUHN, Thomas S. *A estrutura das revoluções científicas*. 5. ed. São Paulo: Perspectiva, 1997.

LEE, Kai-Fu. *Inteligência artificial*. São Paulo: Globo Livros, 2019.

LOSANO, Mario G. *Lições de informática jurídica*. São Paulo: Resenha Tributária, 1974.

MARCACINI, Augusto Tavares Rosa. *Direito e informática: uma abordagem jurídica sobre a criptografia*. Rio de Janeiro: Forense, 2002.

MOREIRA, L. Marco legal da inteligência artificial e segurança digital: perspectivas e desafios. *Revista Brasileira de Direito e Tecnologia*, v. 7, n. 2, p. 89-110, 2024.

MOREIRA, Rômulo de Andrade. A nova lei sobre a tipificação de delitos informáticos: até que enfim um diploma legal necessário. Disponível em: http://jus.com.br. Acesso em: 14 maio 2025.

PIMENTEL, Alexandre Freire. *O direito cibernético: um enfoque teórico e lógico-aplicativo*. Rio de Janeiro: Renovar, 2000.

PINHEIRO, Patrícia Peck. *Direito digital*. 5. ed. ver., atual. e ampl. São Paulo: Saraiva, 2013.

RUSSELL, Stuart; NORVIG, Peter. *Inteligência artificial*. 4. ed. Porto Alegre: AMGH, 2022.

TEIXEIRA, João. *O que é inteligência artificial*. São Paulo: E-galáxia, 2019.

TEPEDINO, Gustavo; DA GUIA SILVA, Rodrigo. Desafios da inteligência artificial em matéria de responsabilidade civil. *Revista Brasileira de Direito Civil*, v. 21, n. 3, p. 61-61, 2019.

VIDAL, Gabriel Rigoldi. Regulação do direito à privacidade na internet: o papel da arquitetura. Disponível em: http://www.jus.com.br/artigos/80369. Acesso em: 14 maio 2025.

VIANNA, Túlio Lima. *Fundamentos de Direito Penal Informática*. Rio de Janeiro: Forense, 2003.