Revista Ibero-Americana de Humanidades, Ciências e Educação — REASE

doi.org/10.51891/rease.v12i5.27332

O USO DE INTELIGÊNCIA ARTIFICIAL NA PRÁTICA CRIMINOSA: A UTILIZAÇÃO DA INTELIGÊNCIA ARTIFICIAL EM DEEPFAKES, FRAUDES FINANCEIRAS E ATAQUES CIBERNÉTICOS E A NECESSIDADE DE IDENTIFICAR LACUNAS NA LEGISLAÇÃO PENAL

Victor Hugo Garbim Oliveira[1]
Luan de Lima Souza[2]
Rodrigo Marcelo de Oliveira Souza[3]

RESUMO: O avanço da inteligência artificial tem provocado profundas transformações na sociedade contemporânea, especialmente no ambiente digital, modificando as formas de comunicação, interação social e circulação de informações. Embora essa evolução tecnológica tenha proporcionado benefícios relevantes em diversas áreas, também passou a ser utilizada como instrumento para a prática de novas modalidades criminosas, marcadas pelo elevado grau de sofisticação, automação e dificuldade de identificação dos responsáveis.Nesse cenário, destacam-se os deepfakes, as fraudes financeiras automatizadas e os ataques cibernéticos contra sistemas públicos e privados, condutas que evidenciam a crescente complexidade da criminalidade digital contemporânea. A utilização de sistemas inteligentes capazes de manipular imagens, reproduzir vozes, automatizar golpes e comprometer infraestruturas essenciais demonstra que a tecnologia ampliou significativamente o alcance e o potencial lesivo das práticas ilícitas. Diante dessa realidade, o Direito Penal brasileiro enfrenta desafios relevantes, uma vez que grande parte de suas normas foi elaborada em contexto anterior à expansão das tecnologias baseadas em inteligência artificial. Assim, surgem dificuldades relacionadas à tipificação das condutas, à responsabilização penal dos envolvidos, à definição dos limites da autoria criminosa e à produção e preservação das provas digitais no processo penal. O presente trabalho tem como objetivo analisar a utilização da inteligência artificial como ferramenta para a prática criminosa, especialmente nos casos envolvendo deepfakes, fraudes financeiras e ataques cibernéticos, bem como discutir as principais lacunas existentes na legislação penal brasileira diante dessas novas formas de criminalidade. Além disso, busca-se refletir sobre a necessidade de atualização legislativa e modernização das instituições responsáveis pela persecução penal, a fim de garantir maior efetividade na proteção dos bens jurídicos tutelados na era digital.

Palavras-chave: inteligência artificial. crimes digitais. deepfake. direito penal. responsabilidade penal

[1]Discente do curso de Direito pela Faculdade Santo Antônio.
[2]Discente do curso de Direito pela Faculdade Santo Antônio.
[3]Professor Orientador do curso de Direito pela Faculdade Santo Antônio.

1. Apresentação do problema real

O tema deste trabalho consiste na análise do uso da inteligência artificial na prática criminosa, especialmente em casos envolvendo deepfakes, fraudes financeiras e ataques cibernéticos, bem como na identificação das lacunas existentes na legislação penal brasileira diante dessas novas modalidades delitivas.

A sociedade contemporânea atravessa uma intensa transformação tecnológica que alterou profundamente a maneira como as pessoas vivem, trabalham e se relacionam. A internet e os recursos digitais deixaram de ocupar posição meramente acessória e passaram a integrar setores essenciais da vida em sociedade, como o sistema financeiro, os meios de comunicação, os serviços de saúde e o próprio Poder Judiciário. Nesse contexto, a inteligência artificial assume papel de destaque por apresentar características inéditas em comparação às tecnologias anteriores, especialmente pela capacidade de simular processos cognitivos humanos, processar grandes volumes de dados em curto espaço de tempo e executar tarefas complexas de forma autônoma.

Entretanto, os avanços proporcionados por essa tecnologia também favoreceram o surgimento de novas práticas criminosas. Ferramentas baseadas em inteligência artificial passaram a ser utilizadas por agentes mal-intencionados para facilitar a execução de delitos, aumentar seu alcance e dificultar a identificação dos responsáveis. Assim, a mesma tecnologia que proporciona eficiência e inovação em diversos setores também se tornou um instrumento relevante para a prática de crimes virtuais cada vez mais sofisticados.

Observa-se, atualmente, uma mudança significativa na dinâmica da criminalidade digital. Se anteriormente os crimes cibernéticos dependiam de atuação manual e conhecimento técnico aprofundado, hoje muitos desses procedimentos foram automatizados por sistemas inteligentes. A criação de vídeos, imagens e áudios falsos com elevado grau de realismo, por exemplo, demonstra como os chamados deepfakes podem ser utilizados para manipular informações, comprometer reputações e induzir vítimas ao erro. Da mesma forma, mecanismos automatizados permitem a realização simultânea de inúmeras fraudes financeiras personalizadas, direcionadas às vulnerabilidades emocionais e econômicas de cada indivíduo. Nesse cenário, o cidadão comum frequentemente encontra dificuldades para identificar que está sendo vítima de um golpe produzido artificialmente por sistemas programados para simular comportamentos humanos com alto nível de precisão.

Diante dessa realidade, surge o problema central analisado neste trabalho: a legislação penal brasileira atualmente vigente é suficiente para enfrentar os crimes praticados mediante o uso de inteligência artificial ou existem lacunas normativas que comprometem a efetiva responsabilização dos agentes? A complexidade dessa discussão decorre, sobretudo, do fato de que o Código Penal brasileiro foi concebido em um contexto histórico voltado predominantemente para crimes praticados no mundo físico, nos quais a conduta humana direta constituía elemento central da infração penal. Em razão disso, o rápido avanço tecnológico contrasta com a lentidão do processo legislativo, criando espaços de incerteza jurídica que podem favorecer situações de impunidade.

Parte-se da hipótese de que a legislação penal brasileira não acompanha, de maneira satisfatória, as transformações decorrentes da evolução tecnológica. Em muitos casos, as respostas estatais limitam-se à ampliação de penas aplicáveis a crimes já existentes, sem considerar que a própria estrutura das condutas criminosas foi modificada pela utilização de sistemas autônomos capazes de aprender, reproduzir padrões e executar tarefas complexas. Como consequência, magistrados e autoridades responsáveis pela persecução penal enfrentam dificuldades ao tentar enquadrar práticas inovadoras em tipos penais elaborados para uma realidade substancialmente distinta.

Dessa forma, o presente artigo busca examinar criticamente as limitações da legislação penal diante do uso da inteligência artificial na prática criminosa, identificando possíveis lacunas normativas e analisando alternativas jurídicas capazes de proporcionar maior proteção à sociedade. Ao mesmo tempo, pretende-se refletir sobre a necessidade de atualização legislativa sem desrespeitar os direitos e garantias fundamentais assegurados pela Constituição Federal.

2. A evolução dos crimes praticados na internet

A compreensão das limitações enfrentadas atualmente pela legislação penal brasileira exige uma análise da evolução histórica dos crimes cibernéticos. O desenvolvimento dessa modalidade criminosa ocorreu de forma gradual e pode ser dividido em diferentes fases, cada uma marcada por características próprias e por distintas formas de utilização da tecnologia para a prática de ilícitos.

Em um primeiro momento, entre o final do século XX e o início dos anos 2000, os crimes digitais concentravam-se principalmente na própria estrutura física ou lógica dos computadores. Nessa fase inicial, o objetivo do agente era comprometer o funcionamento do

sistema informático, destruir arquivos, causar danos operacionais ou inviabilizar o uso da máquina. O computador figurava como alvo direto da conduta criminosa, razão pela qual esses delitos possuíam alcance mais restrito e efeitos limitados, normalmente sem grande repercussão coletiva.

Posteriormente, com a popularização da internet e a ampliação dos serviços digitais, especialmente no setor bancário e financeiro, os crimes virtuais passaram por significativa transformação. O computador deixou de representar exclusivamente o objeto da agressão e passou a funcionar como instrumento para obtenção de vantagens ilícitas, em especial de natureza patrimonial. Foi nesse contexto que se tornaram frequentes práticas como o envio de e-mails fraudulentos, a disseminação de programas maliciosos destinados ao furto de senhas bancárias e outras modalidades de fraude eletrônica.

A reação legislativa brasileira a essa nova realidade ocorreu de maneira relativamente tardia e, em muitos casos, impulsionada pela repercussão social de episódios específicos. Um dos exemplos mais conhecidos foi a promulgação da chamada Lei Carolina Dieckmann, responsável pela inclusão do artigo 154-A no Código Penal, tipificando a invasão de dispositivo informático mediante violação de mecanismo de segurança (*Lei nº 12.737 de 30 de novembro de 2012 (Lei Carolina Dieckmann)*). A construção normativa dessa fase ainda estava voltada à figura do agente que atuava diretamente sobre o sistema, mediante comandos técnicos destinados a superar barreiras de segurança digital.

Entretanto, o cenário atual demonstra uma nova mudança na dinâmica da criminalidade cibernética. A utilização da inteligência artificial e de sistemas automatizados inaugurou uma etapa marcada pela industrialização da prática criminosa. Diferentemente do que ocorria anteriormente, o agente não precisa mais executar pessoalmente todas as etapas do delito nem acompanhar diretamente a vítima durante a fraude. Em muitos casos, basta definir o objetivo pretendido e utilizar plataformas automatizadas capazes de realizar, de forma autônoma, tarefas relacionadas à coleta de dados, produção de mensagens fraudulentas e execução de golpes virtuais.

Essa transformação alterou profundamente a forma de atuação dos criminosos digitais. Enquanto as práticas anteriores dependiam, em grande medida, da habilidade individual do agente para convencer cada vítima separadamente, os sistemas atuais conseguem interagir simultaneamente com milhares de pessoas, adaptando respostas e aperfeiçoando estratégias de convencimento conforme as informações obtidas durante a execução da fraude. Além disso,

determinadas ferramentas conseguem reproduzir padrões de linguagem e comportamento humano com elevado grau de precisão, tornando os golpes mais difíceis de serem identificados.

Como consequência, surgem importantes desafios para o Direito Penal contemporâneo. A utilização de sistemas autônomos na prática criminosa coloca em discussão categorias clássicas relacionadas à autoria, à participação e à própria responsabilização penal. Isso ocorre porque grande parte das estruturas normativas atualmente existentes foi concebida para crimes praticados de maneira direta e pessoal pelo agente humano, realidade que já não corresponde integralmente às novas formas de criminalidade tecnológica.

3. O conflito entre a legislação penal tradicional e as novas tecnologias

3.1. O princípio da legalidade e os limites da interpretação penal

No ordenamento jurídico brasileiro, vigora um dos pilares fundamentais do Direito Penal contemporâneo: o princípio da legalidade estrita. Previsto no artigo 5º, inciso XXXIX, da Constituição Federal e reafirmado pelo artigo 1º do Código Penal, esse princípio estabelece que não há crime nem pena sem previsão legal anterior. Em razão dessa garantia, o magistrado não pode criar tipos penais por interpretação extensiva prejudicial ao acusado nem ampliar o alcance da lei para alcançar condutas que não estejam expressamente previstas no texto normativo.

Embora essa lógica represente importante mecanismo de proteção das liberdades individuais, sua aplicação enfrenta dificuldades diante da rápida evolução tecnológica. Isso ocorre porque grande parte das normas penais brasileiras foi construída em um contexto histórico anterior ao desenvolvimento dos sistemas inteligentes e das novas formas de criminalidade digital.

Um exemplo relevante pode ser observado no artigo 154-A do Código Penal, introduzido pela *Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann*, que passou a tipificar a invasão de dispositivo informático mediante violação indevida de mecanismo de segurança. *(BRASIL, 2012)*. O dispositivo foi elaborado com foco em situações nas quais o agente invade computadores, celulares ou sistemas digitais para obter, adulterar ou destruir dados sem autorização do titular.

Porém, determinadas fraudes contemporâneas não dependem da invasão técnica do aparelho nem da quebra de senhas. Em golpes realizados por meio de inteligência artificial, por exemplo, sistemas de clonagem de voz conseguem reproduzir com elevado grau de fidelidade a

fala de familiares da vítima para solicitar transferências bancárias urgentes. Nesses casos, não há invasão do dispositivo eletrônico, instalação de vírus ou violação de segurança informática. O elemento central da fraude passa a ser a manipulação psicológica da vítima mediante recursos tecnológicos avançados.

Diante dessa situação, a aplicação do artigo 154-A torna-se juridicamente inviável, justamente porque a conduta praticada não corresponde à descrição legal prevista no tipo penal. Em respeito ao princípio da legalidade, o intérprete não pode adaptar artificialmente a norma para alcançar fatos não contemplados expressamente pelo legislador.

Em razão dessas limitações, o Poder Judiciário frequentemente busca enquadrar essas condutas no crime de estelionato eletrônico, previsto no *artigo 171, § 2º-B, do Código Penal*. Entretanto, a estrutura normativa desse dispositivo foi concebida, sobretudo, para fraudes tradicionais realizadas mediante envio de links falsos, páginas fraudulentas ou mensagens eletrônicas enganosas. A legislação não foi construída considerando tecnologias capazes de reproduzir com precisão a voz, a imagem e os padrões comportamentais de terceiros.

Essa lacuna revela um ponto relevante de proporcionalidade e adequação normativa. O grau de sofisticação presente nas fraudes baseadas em inteligência artificial reduz significativamente a possibilidade de percepção do golpe pela vítima, criando uma assimetria técnica muito superior àquela observada nos modelos tradicionais de fraude patrimonial.

Situação semelhante ocorre em relação aos crimes de falsificação documental. Historicamente, os tipos penais relacionados à falsidade material foram estruturados para proteger documentos físicos sujeitos a rasuras, alterações ou supressões materiais. Entretanto, os sistemas de inteligência artificial atuais conseguem produzir identidades falsas, contratos e documentos inteiramente digitais, gerados do zero por softwares avançados, sem qualquer modificação direta em documentos físicos previamente existentes.

Por conta dessas questões, surgem discussões jurídicas acerca da adequação típica dessas condutas aos crimes tradicionalmente previstos no Código Penal. Em muitos casos, argumenta-se que não houve efetiva adulteração material de documento preexistente, mas apenas a criação artificial de um conteúdo inexistente no plano físico. Essa incompatibilidade entre a lógica do Código Penal clássico e a realidade digital contemporânea evidencia a existência de lacunas normativas que dificultam a repressão eficiente dessas práticas.

3.2. A responsabilização penal diante da autonomia dos sistemas inteligentes

No Direito Penal brasileiro, a responsabilização criminal exige não apenas a ocorrência do resultado ilícito, mas também a demonstração do elemento subjetivo da conduta. Isso significa que a condenação depende da comprovação de dolo ou culpa, afastando-se a possibilidade de responsabilização objetiva, atualmente incompatível com as garantias constitucionais do sistema penal brasileiro.

Esse modelo tradicional entra em tensão diante do avanço dos sistemas de inteligência artificial baseados em aprendizado autônomo. Em muitos programas contemporâneos, especialmente nos chamados sistemas de "caixa-preta", o desenvolvedor estabelece apenas parâmetros iniciais e objetivos gerais, sem controlar diretamente as estratégias que serão posteriormente construídas pela própria máquina.

Nesses casos, o sistema desenvolve padrões de comportamento a partir da análise massiva de dados, criando soluções próprias para atingir as metas estabelecidas pelo programador. O problema jurídico surge quando, durante esse processo de aprendizagem, o software passa a adotar práticas ilícitas não previstas originalmente por seu criador.

Imagine-se, por exemplo, um sistema automatizado desenvolvido para operar investimentos no mercado financeiro com o objetivo de maximizar lucros. Durante o processamento de dados disponíveis na internet, a inteligência artificial identifica que notícias falsas influenciam negativamente o valor das ações. A partir dessa constatação, o próprio sistema passa a produzir e divulgar informações fraudulentas para manipular artificialmente o mercado financeiro e obter vantagem econômica.

Nesse cenário, surge uma questão central para o Direito Penal contemporâneo: de que forma seria possível responsabilizar criminalmente o desenvolvedor do software?

Não há, em regra, dolo direto do programador, pois ele não ordenou expressamente a produção de notícias falsas. Da mesma forma, a aplicação do dolo eventual apresenta dificuldades, uma vez que esse instituto exige a previsão concreta do resultado ilícito e a aceitação consciente de sua ocorrência. Em sistemas de inteligência artificial autônoma, muitas vezes o próprio desenvolvedor não consegue prever quais estratégias específicas serão construídas pelo algoritmo ao longo do processo de aprendizagem.

Por outro lado, responsabilizar penalmente o programador apenas em razão do resultado produzido pela máquina equivaleria à adoção de responsabilidade objetiva, hipótese vedada pelo sistema constitucional brasileiro. Entretanto, a completa ausência de responsabilização também

produz consequências problemáticas, especialmente em situações que envolvem graves danos econômicos ou sociais causados por sistemas automatizados.

3.3. A teoria da cegueira deliberada e os limites da responsabilização tecnológica

Diante das dificuldades para comprovar o dolo em crimes praticados com auxílio de inteligência artificial, parte da doutrina defende a aplicação da Teoria da Cegueira Deliberada. Originada no direito norte-americano e utilizada em casos de lavagem de dinheiro, essa teoria busca responsabilizar quem opta conscientemente por ignorar práticas ilícitas para obter benefício econômico.

No contexto tecnológico, ela poderia ser aplicada a desenvolvedores que removem mecanismos de segurança de softwares e disponibilizam sistemas potencialmente perigosos em ambientes clandestinos da internet, assumindo o risco de utilização criminosa da ferramenta.

No entanto, a aplicação dessa teoria exige cautela. A ausência de critérios legais objetivos sobre quais medidas de segurança seriam obrigatórias pode gerar insegurança jurídica e ampliar excessivamente a responsabilização penal. Sem parâmetros claros, falhas técnicas ou limitações inerentes ao desenvolvimento de softwares poderiam ser interpretadas como condutas criminosas, prejudicando a inovação tecnológica e o desenvolvimento científico.

4. Os impactos concretos da criminalidade automatizada

4.1 Deepfakes, dignidade da pessoa humana e violência digital contra mulheres

O avanço da inteligência artificial capaz de criar imagens, vídeos e áudios hiper-realistas trouxe impactos relevantes para a proteção da honra, da imagem e da privacidade, especialmente das mulheres.

Entre as utilizações criminosas mais frequentes estão os deepfakes com conteúdo sexual, produzidos por meio da manipulação de fotografias retiradas de redes sociais para inserir artificialmente o rosto da vítima em vídeos íntimos falsos, divulgados sem consentimento.

A dificuldade jurídica decorre do fato de que parte da legislação penal brasileira foi elaborada considerando a divulgação de conteúdos reais. Assim, algumas interpretações sustentam que materiais produzidos artificialmente não configurariam exatamente uma "cena real", mas uma criação digital inexistente no plano físico.

Embora isso não impeça necessariamente a responsabilização criminal, evidencia a insuficiência de tipos penais criados antes da popularização das tecnologias de manipulação sintética de imagem.

Além das violações individuais, os deepfakes também representam ameaça à confiança nas instituições públicas. A capacidade de reproduzir artificialmente a imagem e a voz de autoridades, magistrados e agentes políticos pode comprometer a credibilidade institucional e afetar a estabilidade democrática. Nesse cenário, a proteção jurídica ultrapassa a esfera da honra individual e alcança valores relacionados à segurança institucional e à confiança pública.

4.2. O modelo de "*crime como serviço*" nas fraudes bancárias digitais

Os crimes patrimoniais praticados pela internet passaram por significativa transformação com o surgimento do modelo conhecido como crime as a service (CaaS), caracterizado pela comercialização de ferramentas tecnológicas destinadas à prática de fraudes digitais.

Nesse sistema, grupos especializados desenvolvem softwares automatizados baseados em inteligência artificial e disponibilizam essas ferramentas para terceiros mediante pagamento ou participação nos lucros obtidos com os golpes. A dinâmica funciona de forma semelhante a uma estrutura empresarial, na qual alguns agentes criam os sistemas e outros executam diretamente as fraudes.

Com isso, os golpes virtuais tornaram-se mais sofisticados. Os sistemas conseguem manter conversas naturais com vítimas, utilizar linguagem técnica semelhante à de instituições financeiras e simular atendimentos bancários, aumentando a credibilidade da fraude e dificultando sua identificação.

No âmbito jurídico-penal, surge a dificuldade de definir os limites da responsabilidade de cada participante da cadeia criminosa. Em estruturas automatizadas e descentralizadas, torna-se complexo identificar até que ponto o desenvolvedor do sistema responde pelos crimes praticados por terceiros que utilizaram a ferramenta.

Além disso, a rapidez das transações digitais dificulta a investigação criminal, já que os valores desviados costumam ser transferidos instantaneamente entre diversas contas intermediárias. Esse cenário demonstra que as categorias tradicionais de coautoria e participação nem sempre conseguem responder adequadamente à criminalidade digital contemporânea.

4.3. O ransomware e os ataques automatizados contra serviços essenciais

Outro risco relevante relacionado ao uso criminoso da inteligência artificial envolve ataques cibernéticos direcionados contra serviços públicos e estruturas essenciais, como hospitais, órgãos administrativos e sistemas do Poder Judiciário.

Diferentemente das invasões tradicionais, os ataques atuais operam de forma silenciosa e automatizada. Sistemas maliciosos conseguem permanecer ocultos nas redes por longos períodos, analisando padrões de funcionamento, horários de menor vigilância e vulnerabilidades da infraestrutura digital.

Após essa fase, os programas executam ataques do tipo ransomware, caracterizados pelo bloqueio ou criptografia de dados mediante exigência de pagamento para liberação do acesso. Em muitos casos, o próprio sistema identifica os arquivos mais importantes e define valores compatíveis com a capacidade financeira da vítima, aumentando as chances de pagamento do resgate.

Os prejuízos causados ultrapassam a esfera patrimonial. Quando atingem hospitais, tribunais ou órgãos públicos, esses ataques comprometem serviços essenciais e colocam em risco direitos fundamentais da coletividade, como o acesso à saúde e a continuidade dos serviços públicos.

Também surgem dificuldades no enquadramento jurídico dessas condutas. Embora exista aproximação com o crime de extorsão previsto no artigo 158 do Código Penal, a legislação foi construída considerando ameaças diretas contra a pessoa, enquanto os ataques automatizados utilizam a paralisação digital de sistemas como forma de coerção.

5. A crise probatória e os desafios do processo penal na era digital

O avanço das tecnologias de manipulação digital alterou não apenas a prática dos crimes, mas também a forma de produção e análise das provas no processo penal.

Durante muito tempo, fotografias, vídeos e gravações de áudio foram considerados meios de prova altamente confiáveis, devido à presunção de autenticidade atribuída aos registros audiovisuais. Contudo, o desenvolvimento de deepfakes altamente realistas modificou essa lógica, criando um cenário de insegurança probatória que afeta diretamente a efetividade do processo penal.

A principal preocupação está na possibilidade de acusados alegarem que gravações legítimas seriam montagens produzidas artificialmente. Em determinados casos, a simples dúvida sobre a autenticidade do material pode comprometer sua força probatória.

Como consequência, o Ministério Público e os órgãos de investigação passaram a depender cada vez mais de perícias técnicas especializadas para comprovar a integridade dos arquivos digitais. A dificuldade aumenta com a rápida evolução dos sistemas de inteligência artificial, que tornam as falsificações cada vez mais sofisticadas.

Seguindo esse contexto, torna-se necessária a modernização dos mecanismos de preservação da cadeia de custódia da prova digital previstos no Código de Processo Penal, já que a simples guarda de arquivos eletrônicos não garante autenticidade e confiabilidade.

Por isso, diversos estudiosos defendem a utilização de certificação digital, registros criptográficos imutáveis e sistemas avançados de autenticação desde a coleta da prova. Sem a modernização técnica das instituições responsáveis pela persecução penal, cresce o risco de impunidade, fragilidade probatória e erros judiciais relacionados à manipulação de evidências digitais.

6. Regulação, modernização legislativa e os desafios do Direito Penal na era da inteligência artificial

O avanço da inteligência artificial aplicada à prática criminosa evidenciou as limitações da legislação penal brasileira diante das novas formas de criminalidade digital. As estruturas tradicionais do Código Penal e do Código de Processo Penal, elaboradas em um contexto voltado para crimes praticados no mundo físico, mostram dificuldades para enfrentar condutas automatizadas, descentralizadas e executadas por sistemas tecnológicos autônomos.

Por conta disso, surgem diferentes posições sobre a forma de atuação do Estado. Parte da doutrina entende que as normas atuais ainda seriam suficientes, desde que interpretadas de maneira adaptada às novas tecnologias. Outra corrente, contudo, sustenta que os crimes praticados mediante inteligência artificial possuem características próprias e, por isso, exigem atualização legislativa específica.

A experiência prática demonstra que respostas legislativas improvisadas, limitadas apenas ao aumento de penas ou à criação apressada de novos tipos penais, não solucionam adequadamente o problema. Em alguns casos, isso acaba produzindo desequilíbrios no sistema punitivo e comprometendo a proporcionalidade das sanções penais.

Seguindo esse contexto, ganha relevância o debate relacionado ao Projeto de Lei nº 2.338/2023, destinado à criação do Marco Legal da Inteligência Artificial no Brasil. O projeto propõe um modelo regulatório baseado em níveis de risco, estabelecendo deveres de transparência, fiscalização e controle para sistemas classificados como de alto risco.

A aproximação entre regulação tecnológica e Direito Penal pode representar um caminho mais adequado para enfrentar a criminalidade digital contemporânea. A violação consciente de deveres de segurança, auditoria e controle de sistemas automatizados pode servir como parâmetro relevante para a responsabilização jurídica de desenvolvedores e empresas de tecnologia.

Apesar disso, torna-se necessária a criação de tipos penais específicos voltados à fraude por simulação identitária, especialmente em situações envolvendo clonagem de voz, manipulação de imagem e utilização indevida de dados biométricos por meio de inteligência artificial. A construção de normas mais precisas contribuiria para reduzir lacunas legislativas e ampliar a segurança jurídica.

Ao longo desta pesquisa, verificou-se que o enfrentamento dessa nova modalidade de criminalidade não pode ser resolvido apenas com o endurecimento das penas. O problema exige modernização legislativa, fortalecimento técnico das instituições responsáveis pela persecução penal e atualização dos mecanismos de produção e preservação de provas digitais.

No plano processual, também se mostra indispensável o investimento em estrutura técnica, perícia especializada e mecanismos modernos de autenticação de provas eletrônicas, sob pena de aumento da impunidade e fragilidade do sistema de justiça criminal.

Por fim, conclui-se que o principal desafio do Direito Penal contemporâneo consiste em adaptar-se às transformações tecnológicas sem afastar os princípios constitucionais que sustentam o Estado Democrático de Direito. O equilíbrio entre inovação legislativa, segurança jurídica e proteção das garantias fundamentais será essencial para que o sistema penal brasileiro permaneça eficaz diante das novas formas de criminalidade digital.

7. CONSIDERAÇÕES FINAIS

Ao longo deste trabalho, buscamos analisar os impactos do uso da inteligência artificial na prática criminosa e os desafios que essas novas tecnologias têm causado ao Direito Penal brasileiro. Foi possível perceber que ferramentas como deepfakes, fraudes automatizadas e

ataques cibernéticos vêm transformando a dinâmica da criminalidade digital, tornando os delitos mais sofisticados e difíceis de serem combatidos.

Durante a pesquisa, constatamos que a legislação penal brasileira ainda apresenta limitações para lidar adequadamente com determinadas condutas praticadas por meio de sistemas inteligentes. Além disso, observamos que o avanço tecnológico também afeta diretamente a produção de provas, a responsabilização penal e a atuação das instituições responsáveis pela investigação e julgamento desses crimes.

Entendemos que o enfrentamento da criminalidade tecnológica exige não apenas atualização legislativa, mas também investimentos em capacitação técnica, modernização das investigações e fortalecimento dos mecanismos de preservação das provas digitais. Ao mesmo tempo, consideramos fundamental que qualquer mudança ocorra em conformidade com os princípios constitucionais e com as garantias fundamentais asseguradas pelo ordenamento jurídico brasileiro.

Por fim, concluímos que a relação entre inteligência artificial e Direito Penal representa um dos grandes desafios jurídicos da atualidade. Por essa razão, acreditamos ser indispensável a construção de soluções capazes de acompanhar a evolução tecnológica sem comprometer a segurança jurídica, a proteção dos direitos fundamentais e a estabilidade das instituições democráticas.

REFERÊNCIAS BIBLIOGRÁFICAS E DOCUMENTAIS

ARTIGO 154-A do Código Penal – Legislação Atualizada.

BRASIL. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Senado Federal, 1988. Disponível em: Planalto. Acesso em: 22 maio 2026.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. Brasília, DF: Presidência da República, 1940. Disponível em: Código Penal – Planalto. Acesso em: 22 maio 2026.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos e altera o Código Penal. Brasília, DF: Presidência da República, 2012. Disponível em: Lei 12.737/2012 – Planalto. Acesso em: 22 maio 2026.

BRASIL. Lei nº 14.155, de 27 de maio de 2021. Altera o Código Penal para tornar mais graves os crimes de invasão de dispositivo informático e estelionato eletrônico. Brasília, DF: Presidência da República, 2021. Disponível em: Lei 14.155/2021 – Planalto. Acesso em: 22 maio 2026.

BRASIL. Projeto de Lei nº 2.338/2023. Dispõe sobre o uso da Inteligência Artificial no Brasil. Senado Federal, 2023. Disponível em: PL 2338/2023 – Senado Federal. Acesso em: 22 maio 2026.

CRESPO, Marcelo Xavier de Freitas. Crimes digitais. São Paulo: Saraiva, 2011.

LEI Carolina Dieckmann – Informática Jurídica.

LEI nº 12.737/2012 – Senado Federal.

PECK, Patricia. Direito digital. São Paulo: Saraiva, 2022.