UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE CIÊNCIAS JURÍDICAS
FACULDADE DE DIREITO DO RECIFE

IGOR VINÍCIUS GUERRA RÊGO DUARTE

FRAUDES ELETRÔNICAS ASSISTIDAS POR INTELIGÊNCIAS ARTIFICIAIS: análise da tipicidade com base na lei Nº 14.155 DE 2021

Recife

2024

IGOR VINÍCIUS GUERRA RÊGO DUARTE

FRAUDES ELETRÔNICAS ASSISTIDAS POR INTELIGÊNCIAS ARTIFICIAIS: análise da tipicidade com base na lei Nº 14.155 DE 2021

Trabalho de conclusão de curso apresentado como requisito parcial para a obtenção do grau de Bacharel em Direito pela Universidade Federal de Pernambuco.
Área de Concentração: Direito Penal.
Orientador: Prof. Dr. Teodomiro Noronha Cardozo.

Recife

2024

V785f Vinícius Guerra Rêgo Duarte, Igor

FRAUDES ELETRÔNICAS ASSISTIDAS POR INTELIGÊNCIAS ARTIFICIAIS: / Igor Vinícius Guerra Rêgo Duarte. – Brasília: Escola Superior do Ministério Público da União, 2024.

38f.

Trabalho de conclusão de curso (DIREITO) – Escola Superior do Ministério Público da União: Brasília, 2024.

Orientador(a): Dr. Teodomiro Noronha Cardozo

1. Inteligência Artificial. 2. Direito penal. 3. Tipicidade Formal. 4. Tecnologia. I. Título.

Ficha catalográfica elaborada automaticamente, com os dados fornecidos pelo(a) autor(a)

IGOR VINÍCIUS GUERRA RÊGO DUARTE

FRAUDES ELETRÔNICAS ASSISTIDAS POR INTELIGÊNCIAS ARTIFICIAIS: análise da tipicidade com base na lei Nº 14.155 DE 2021

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Direito da Universidade Federal de Pernambuco, como requisito parcial para obtenção do título de bacharel em Direito.

Aprovado em: 16/10/2024

BANCA EXAMINADORA

_____

Prof. Dr. Teodomiro Noronha Cardozo (Orientador)

Universidade Federal de Pernambuco

_____

Prof. Dra. Eleonora de Souza Luna (Examinadora Interna)

Universidade Federal de Pernambuco

_____

Prof. Dr. Paulo Simplício Bandeira (Examinador Interno)

Universidade Federal de Pernambuco

RESUMO

O presente trabalho de conclusão de curso aborda o tema "Fraudes Eletrônicas Assistidas por Inteligência Artificial: Análise da Tipicidade Formal com Base na Lei nº 14.155 de 2021". Estruturado em três capítulos, o estudo visa investigar se as fraudes cometidas com o uso de inteligência artificial podem ser enquadradas no § 2º-A do artigo 171 do Código Penal, por meio de uma interpretação analógica da expressão "qualquer outro meio fraudulento análogo". A pesquisa busca analisar a suficiência da legislação vigente para tratar dessas condutas, considerando as particularidades tecnológicas das fraudes envolvendo IA. Na elaboração deste trabalho, utilizou-se o método hipotético-dedutivo, no qual a hipótese formulada foi submetida ao teste de falseabilidade, através da análise de doutrinas e legislação. O primeiro capítulo discute os fundamentos do crime de estelionato e acréscimos da Lei nº 14.155 de 2021. O segundo capítulo destaca elementos doutrinários necessários para a análise da tipicidade formal. O terceiro capítulo analisa a possibilidade de enquadramento jurídico dessas fraudes por meio de uma interpretação analógica do § 2º-A do artigo 171, investigando a necessidade de uma atualização legislativa para lidar com os novos desafios impostos pela tecnologia.

Palavras-Chave: Inteligência Artificial; Direito penal; Tipicidade Formal; Tecnologia.

ABSTRACT

The present final course paper addresses the topic "Artificial Intelligence-Assisted Electronic Fraud: Analysis of Formal Typicity Based on Law No. 14.155 of 2021." Structured in three chapters, the study aims to investigate whether fraud committed using artificial intelligence can be framed under § 2º-A of Article 171 of the Penal Code through an analogical interpretation of the expression "any other analogous fraudulent means." The research seeks to analyze the sufficiency of the current legislation in addressing these conducts, considering the technological particularities of fraud involving AI. The hypothetical-deductive method was applied in this study, where the formulated hypothesis was subjected to falsifiability testing through the analysis of legal doctrines and legislation. The first chapter discusses the foundations of the crime of fraud and the additions brought by Law No. 14.155 of 2021. The second chapter highlights the doctrinal elements necessary for the analysis of formal typicity. The third chapter analyzes the possibility of legally framing these frauds through an analogical interpretation of § 2º-A of Article 171, investigating the need for legislative updates to address the new challenges posed by technology.

Keywords: Artificial Intelligence; Criminal Law; Formal Typicity; Technology.

SUMÁRIO

1 INTRODUÇÃO

1.1 Problemática

As fraudes eletrônicas instituídas pelo § 2º-A do Código Penal, introduzido pela Lei nº 14.155 de 2021, envolvem expressamente o uso de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento. Esse tipo penal demonstra-se de extrema importância para combater a escalada dessa prática criminosa na realidade atual brasileira. A problemática surge do destaque que o legislador deu a três espécies principais (uso de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento), levantando a discussão sobre quais outras espécies podem ser enquadradas na parte final do tipo que tipifica "qualquer outro meio fraudulento análogo".

Essa escalada de fraudes eletrônicas não se limita às três espécies principais, mas tem sido cometida por diversos meios. Entre eles, destacam-se as fraudes realizadas com a utilização de inteligência artificial (IA). Esse tipo de fraude não se enquadra de forma expressa nos tópicos trazidos pelo tipo penal, mas existe a possibilidade de ser incluído na parte final do artigo, que menciona a utilização de "qualquer outro meio fraudulento análogo".

O presente trabalho de conclusão de curso dedica-se à investigação da tipicidade formal das fraudes eletrônicas assistidas por IA, especialmente no contexto da Lei nº 14.155, de 2021, verificando a possibilidade de enquadramento da fraude utilizando IA no novo § 2º-A, do artigo 171 do Código Penal.

Essa análise demanda a compreensão do caráter tripartido do crime no Brasil, sendo necessária uma avaliação da tipicidade formal. Nessa análise específica, a tipicidade formal exigirá uma compreensão aprofundada da interpretação análoga do tipo penal e seus limites legais. Tal entendimento facilitará a reflexão sobre a possibilidade de o uso de inteligência artificial ser elemento suficiente para caracterizar uma fraude eletrônica, conforme a Lei nº 14.155, de 2021.

A necessidade dessa análise surge com o rápido avanço tecnológico e o crescente uso da IA em diversas áreas, inclusive em práticas fraudulentas. Embora a regulamentação dos crimes envolvendo IA ainda esteja em fase de desenvolvimento, é crucial reconhecer que, apesar da autonomia tecnológica, as ações da IA são sempre direcionadas por seres humanos, que podem utilizá-la para fins ilícitos.

Este estudo examina se a legislação vigente, com ênfase na Lei nº 14.155, de 2021, é suficiente para lidar com as fraudes cometidas com o uso de IA e se há necessidade de ajustes para enfrentar os novos desafios impostos por essa tecnologia.

1.1.1 Hipótese da pesquisa

A necessidade de definir, no âmbito da tipicidade formal, se as fraudes eletrônicas realizadas com o uso de inteligência artificial podem ser adequadamente enquadradas no § 2º-A do artigo 171 do Código Penal, por meio de uma interpretação analógica da expressão "qualquer outro meio fraudulento análogo", considerando as especificidades tecnológicas dessas condutas e a forma como a legislação vigente realiza a análise da tipicidade formal.

1.1.2 Pergunta preliminar

A legislação penal brasileira, em especial o § 2º-A do artigo 171 do Código Penal, abarca fraudes eletrônicas assistidas por inteligência artificial, ou seria necessário um aprimoramento legal para lidar com as especificidades tecnológicas dessas novas formas de fraude?

1.1.3 Resposta preliminar

Sim, é possível enquadrar as fraudes eletrônicas assistidas por inteligência artificial no § 2º-A do artigo 171 do Código Penal, por meio de uma interpretação analógica da expressão "qualquer outro meio fraudulento análogo". A tipicidade formal das condutas fraudulentas realizadas com o uso de IA pode ser acomodada

dentro da legislação vigente, visto que a redação final do artigo permite abranger novas tecnologias utilizadas para fins ilícitos. Ao considerar a complexidade e a sofisticação dos mecanismos de IA, uma inovação legislativa seria desejável para trazer maior clareza jurídica e estabelecer um tratamento específico para esses crimes. Esse aprimoramento legislativo poderia não apenas delimitar de forma precisa os elementos constitutivos da fraude por IA, mas também agravar as penas, levando em consideração o maior potencial de danos e a dificuldade de detecção dessas condutas ilícitas. Essa mudança permitiria uma melhor adaptação do ordenamento jurídico à realidade tecnológica, garantindo maior efetividade na prevenção e repressão desses crimes.

1.2 Metodologia

Para o desenvolvimento deste trabalho de conclusão de curso, adotar-se-á o método hipotético-dedutivo de Karl Popper, que pressupõe a formulação de uma hipótese e sua posterior testagem por falseabilidade. A hipótese central é a de que as fraudes eletrônicas assistidas por inteligência artificial podem ser enquadradas no § 2º-A do artigo 171 do Código Penal, por meio de uma interpretação analógica. Essa hipótese será submetida ao processo de falseabilidade, por meio de análise crítica e jurídica, a fim de verificar sua validade e consistência diante das evidências e da legislação vigente.

Esse objetivo será atingido através de uma revisão bibliográfica abrangente, contemplando uma ampla variedade de fontes, como artigos científicos, monografias, dissertações de mestrado e periódicos especializados. A revisão visa explorar o desenvolvimento e a aplicação de normas que regulam fraudes eletrônicas e crimes relacionados à inteligência artificial, tanto no contexto brasileiro quanto em legislações internacionais, buscando fornecer uma base teórica robusta para a análise proposta.

1.3 Objetivo geral

Analisar se as fraudes eletrônicas assistidas por inteligência artificial podem

ser enquadradas no § 2º-A do artigo 171 do Código Penal, por meio de uma interpretação analógica da expressão "qualquer outro meio fraudulento análogo", considerando as especificidades tecnológicas dessas condutas e a maneira que a legislação vigente realiza a análise da tipicidade formal.

1.4 Objetivos específicos

1.4.1 Examinar os elementos da tipicidade formal no crime de estelionato, com foco na aplicação da Lei nº 14.155, de 2021, e sua relação com fraudes eletrônicas.

1.4.2 Analisar as particularidades das fraudes eletrônicas assistidas por inteligência artificial e suas diferenças em relação às fraudes tradicionais previstas na legislação penal.

1.4.3 Avaliar se, por meio da interpretação analógica, as fraudes eletrônicas assistidas por inteligência artificial podem ser enquadradas como 'meio fraudulento análogo' no § 2º-A do artigo 171 do Código Penal.

1.5 Justificativa

Este trabalho de conclusão de curso busca investigar se as fraudes eletrônicas assistidas por inteligência artificial podem ser adequadamente enquadradas no § 2º-A do artigo 171 do Código Penal, por meio de uma interpretação analógica da expressão "qualquer outro meio fraudulento análogo". A relevância desse estudo está diretamente ligada ao crescimento exponencial do uso de IA para finalidades fraudulentas, o que levanta importantes questionamentos sobre a suficiência da legislação penal vigente para lidar com essas novas formas de fraude.

Realizar este estudo é essencial para determinar se o atual enquadramento penal é eficaz para combater fraudes com IA ou se é necessária uma inovação legislativa que aborde de forma específica os desafios trazidos por essa tecnologia. Essa análise contribuirá para a melhora do sistema penal, tornando-o capaz de oferecer uma resposta adequada às novas modalidades de crimes tecnológicos.

2 FRAUDE ELETRÔNICA E INTELIGÊNCIA ARTIFICIAL

2.1 Estelionato e a Lei nº 14.155 de 2021

O *stellionatus* era, no período do império Romano, incriminado de forma genérica, abrangendo todos os tipos de fraude não previstos explicitamente na legislação (Prado, 2019). Esse tratamento amplo demonstra uma tendência histórica de adaptar a legislação para combater as diferentes formas de engano e fraude, que surgem conforme o contexto econômico e social evolui. Com o tempo, essa abordagem abrangente permaneceu essencial, especialmente diante da inovação contínua nas técnicas de fraude.

O Código Penal Brasileiro, em seu artigo 171, *caput*, define o estelionato como "obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil ou qualquer outro meio fraudulento". O bem jurídico protegido por essa norma é o patrimônio, sendo o núcleo central do tipo penal o verbo "obter", que remete ao ato de alcançar vantagem indevida. Conforme sustenta Prado, qualquer pessoa pode ser o sujeito ativo ou passivo no crime de estelionato em sua modalidade genérica.

Ao destacar que a conduta nuclear do tipo é o verbo“obter”, Bitencourt defende que esse núcleo exige a produção de dois resultados específicos: a vantagem ilícita e o prejuízo alheio. Esse duplo resultado é tratado pelo autor da seguinte forma:

> Para a configuração do estelionato é indispensável que o agente obtenha proveito indevido em prejuízo alheio. Exige o tipo penal a produção de duplo resultado (vantagem ilícita e prejuízo alheio), que examinaremos logo a seguir. (...) A duplicidade de nexo causal está representada por dupla relação de causa e efeito; num primeiro momento, funciona a fraude como causa, e o engano decorrente do ardil, como efeito; no momento subsequente, o erro consequente do engano, como causa, e a obtenção da vantagem indevida e o dano patrimonial correspondente406 (esses dois representando a segunda duplicidade). Trata-se, com efeito, de crime de resultado duplo, uma vez que para se consumar exige a obtenção de vantagem ilícita, de um lado, e a ocorrência efetiva de um prejuízo para a

> vítima, de outro. A ausência de qualquer desses resultados descaracteriza o estelionato consumado, restando, em princípio, a figura da tentativa. (Bitencourt, 2020, página 447)

A obtenção da vantagem indevida ocorre quando o agente cria a situação de engano ou se aproveita de um erro já existente. Essa conduta pode ser praticada de diversas formas, mas sempre com a intenção de gerar prejuízo à vítima e obter um ganho ilícito. Nucci, ao tratar sobre o estelionato defende que:

> "Induzir" significa incutir ou persuadir, enquanto "manter" significa conservar ou fazer permanecer. Portanto, a obtenção da vantagem indevida ocorre quando o agente leva a vítima ao erro ou permite que ela permaneça na situação de engano na qual se envolveu sozinha. É possível que o autor do estelionato provoque a situação de engano ou apenas se aproveite dela (Nucci, 2023, pág 1267).

O elemento subjetivo do crime de estelionato é o dolo, ou seja, a intenção consciente do agente em obter lucro indevido. O tipo penal também é caracterizado pela presença de três elementos importantes: o "erro", que é a distorção da percepção da vítima; o "artifício", que consiste em uma alteração enganosa da verdade; e o "ardil", que envolve um plano fraudulento mais elaborado, demonstrando astúcia na execução. Esses elementos são usados pelo agente para manipular a vítima, levando-a a acreditar em algo que não corresponde à realidade.

Essas três possibilidades são as centrais no tipo penal, mas o legislador também tipifica a conduta que que utilize “qualquer meio fraudulento análogo”. Segundo Luiz Régis Prado, essa tipificação deixa margem para aplicação de uma interpretação analógica. Nas palavras do autor:

> Além da enumeração exemplificativa – artifício ou ardil –, o legislador utiliza-se da fórmula genérica qualquer outro meio fraudulento, dando margem ao emprego de interpretação analógica. A interpretação analógica (intra legem), espécie do gênero interpretação extensiva, abrange os casos análogos, conforme fórmula casuística gravada no dispositivo legal. Destarte, qualquer conduta dolosa do agente, revestida de fraude, que tenha levado o sujeito passivo a incorrer ou a manter-se em erro, com a obtenção da vantagem ilícita e a consequente lesão patrimonial, amolda-se ao tipo em epígrafe, salvo situações especiais que ensejam o deslocamento da tipicidade para outras normas incriminadoras (Prado, 2019, pág. 687).

A prática do estelionato aumentou significativamente ao longo dos séculos,

especialmente com a complexidade crescente das transações econômicas e das relações negociais. O legislador, buscando preservar a integridade dessas relações, ampliou a proteção do patrimônio, adaptando o tipo penal de estelionato para abranger novas formas de fraude (Prado, 2019).

A expansão das tecnologias digitais trouxe consigo uma nova modalidade de fraude, mais sofisticada e abrangente, revelando uma lacuna nas legislações penais tradicionais. A manipulação de dados, o uso de informações pessoais de forma ilícita e outros crimes virtuais não eram previstos expressamente pela legislação anterior, o que exigiu a criação de um novo dispositivo legal.

Muitas legislações modernas já contemplam crimes cometidos por meio de tecnologias informáticas. O Direito Penal português, por exemplo, prevê, no artigo 221.1 de seu Código Penal, a "burla informática", que abrange fraudes realizadas por interferência no processamento de dados, manipulação incorreta de programas de computador ou uso não autorizado de dados.

O legislador português reconhece que as novas formas de fraude, facilitadas pela tecnologia, exigem respostas mais específicas e rigorosas para proteger o patrimônio e coibir práticas ilícitas. Essa evolução normativa também é observada em outras jurisdições, que buscam adaptar suas legislações às exigências da era digital.

Essa adaptação também é percebida, por exemplo, no Direito Espanhol. Luiz Regis Prado destaca o artigo da legislação espanhola e comenta sobre a mesma:

> De modo similar, o Código Penal espanhol pune como autor de estelionato aquele que, com ânimo de lucro e valendo-se de alguma manipulação informática ou artifício semelhante, consiga a transferência não consentida de qualquer ativo patrimonial em prejuízo de terceiro (art. 248).45 “Artículo 248. 1. Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno. 2. También se consideran reos de estafa: a) Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro. b) Los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo. c) Los que utilizando tarjetas de crédito o débito, o cheques de

> viaje, o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero (Prado, 2019, pág. 689).

O Brasil também precisou atualizar suas previsões legais diante do aumento expressivo dos crimes digitais. Esse enfrentamento teve início com a Lei Carolina Dieckmann (Lei 12.737/2012) e depois seguiu com a promulgação do Marco Civil da Internet (Lei 12.965/2014). Esses esforços incipientes culminaram na Lei 14.155/2021, objeto de análise do presente trabalho. Essa lei inseriu o § 2º-A no artigo 171, prevendo penas mais severas para as fraudes eletrônicas, uma vez que a legislação anterior não previa penas proporcionais à gravidade desses crimes.

O aumento exponencial de golpes digitais, como phishing e ligações falsas, evidenciou a necessidade de adaptar o ordenamento jurídico. As fraudes digitais, mais difíceis de rastrear e com maior potencial de disseminação, exigiram uma resposta mais severa do legislador. A promulgação do § 2º-A do artigo 171 reflete essa preocupação, buscando garantir que o direito penal se mantenha eficaz na proteção ao patrimônio frente às novas modalidades de estelionato.

Ao tratar sobre a necessidade de tipificação das Fraudes Eletrônicas, o anuário brasileiro de segurança pública de 2023 revela que:

> A tipificação da fraude eletrônica foi uma tentativa do legislador de dar resposta ao crescimento vertiginoso das práticas criminosas através de redes sociais e aplicativos de mensagem. Entre 2018 e 2022 os crimes de estelionato registrados pelas Polícias Civil cresceram 326,3%, passando de 426.799 casos em 2018 para 1.819.409 em 2022 (Anuário Brasileiro de Segurança Pública, 2023, pág. 94).

Ao ampliar o alcance da lei e prever penas mais rigorosas para fraudes eletrônicas, a legislação brasileira passou a se alinhar com as práticas internacionais, reconhecendo que o ambiente digital é um espaço suscetível a ações ilícitas. A adaptação das normas penais para lidar com fraudes que muitas vezes transcendem fronteiras é uma necessidade crescente, dado o caráter global e descentralizado das fraudes digitais, que desafiam as capacidades tradicionais de investigação e repressão.

2.2 Fraudes eletrônicas no artigo 171 do Código Penal

O § 2º-A do artigo 171 do Código Penal, mesmo estando inserido no contexto do crime de estelionato, é uma qualificadora que trata especificamente de fraudes eletrônicas. Sua introdução pela Lei nº 14.155 em 27 de maio de 2021 reflete a preocupação do legislador em estabelecer penas mais rigorosas para as fraudes praticadas por meio digital, com a pena de reclusão variando de quatro a oito anos, além de multa. O anuário brasileiro de segurança pública destaca a importância dessa tipificação da seguinte forma:

> O crime de estelionato em meio eletrônico foi tipificado apenas em 27 de maio de 2021, pela Lei n° 14.155/2021. Algumas UF já conseguem realizar sua mensuração. Embora com limitações, como o fato de que 9 estados não terem informado os dados, neste primeiro levantamento foi possível identificar que, em 2021, foram registrados 60.590 casos de estelionato por fraude eletrônica (Anuário brasileiro de segurança pública, 2022, pág. 120).

O legislador delineou a caracterização dessas fraudes da seguinte forma:

> Art. 171 - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento: Pena - reclusão, de um a cinco anos, e multa, de quinhentos mil réis a dez contos de réis. (Vide Lei nº 7.209, de 1984) (...) Fraude eletrônica § 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo (Incluído pela Lei nº 14.155, de 2021) (Código Penal, Artigo 171, § 2º-A).

O tipo penal faz menção a três meios principais pelos quais as fraudes eletrônicas podem ser cometidas: redes sociais, contatos telefônicos e e-mails fraudulentos. Esses conceitos são amplamente utilizados no contexto digital, e cada um tem características específicas que permitem sua aplicação na prática de fraudes. Essas modalidades já estavam presentes na realidade brasileira e , à época, já figuravam como as fraudes eletrônicas com crescimento exponencial, conforme destaca o Anuário Brasileiro de Segurança Pública de 2023:

> Ao contrário do que ocorreu na maioria dos roubos e furtos, que apresentaram queda acentuada na pandemia, os estelionatos via redes sociais e aplicativos de mensagens tiveram crescimento exponencial em

> vários países do mundo (Naidoo, 20204 ; Buil-Gil et al, 20205 ; Chawki, 20216) (Anuário brasileiro de segurança pública, 2023, página 94).

Redes sociais são plataformas digitais que permitem a interação entre usuários por meio da criação e compartilhamento de conteúdo, como textos, imagens e vídeos. Exemplos de redes sociais incluem Facebook, Instagram, Twitter e LinkedIn. No contexto das fraudes eletrônicas, as redes sociais são frequentemente usadas para criar perfis falsos ou contas falsas que se passam por pessoas ou empresas legítimas. Os golpistas entram em contato com as vítimas, se passando por amigos ou representantes de instituições financeiras, induzindo-as a fornecer informações pessoais ou financeiras. A ação através de redes sociais é feita através de diversas modalidades, inclusive sem que o usuário disponibilize seus dados, conforme destaca:

> Os golpes através de redes sociais e aplicativos de mensagens também podem ser operados sem que o usuário disponibilize seus dados financeiros. Tem sido cada vez mais comuns os casos de estelionato sentimental, modalidade de golpe em que o autor estabelece uma relação amorosa com a vítima – que pode ser apenas virtual -, e obtém vantagens financeiras (Assenção e Pereira, 20237) (Anuário brasileiro de segurança pública, 2023, pág. 95).

Contatos telefônicos referem-se ao uso de chamadas telefônicas ou mensagens de texto para enganar a vítima. Isso pode incluir tanto ligações diretas quanto o envio de mensagens SMS. Fraudes telefônicas, também conhecidas como vishing (voice phishing), são comuns e envolvem a criação de cenários fraudulentos, como supostos bloqueios de contas bancárias ou ofertas de prêmios inexistentes, para induzir a vítima a fornecer seus dados ou realizar transferências de dinheiro.

E-mails fraudulentos, também conhecidos como phishing, são mensagens eletrônicas disfarçadas de comunicação legítima, normalmente de empresas ou instituições conhecidas, como bancos, provedores de serviço ou órgãos governamentais. O objetivo é enganar o destinatário para que ele clique em links maliciosos, baixe arquivos perigosos ou forneça informações confidenciais, como senhas e números de cartão de crédito.

O estelionato digital, assim como o tradicional, baseia-se na utilização de fraude (artifícios, ciladas ou enganos) para manipular a vítima de tal forma que ela acredite estar realizando uma transação vantajosa ou um negócio promissor. A pessoa ofendida, sob erro, entrega voluntariamente o bem sugerido pelo agente criminoso ou, no contexto eletrônico, as informações que permitem acessar tais bens (Nucci, 2023).

Esse tipo de fraude não é bem sucedida apenas com base na desinformação e despreparo das vítimas, mas através de uma especialização dos indivíduos que se aproveitam das novas possibilidades criadas pelo desenvolvimento tecnológico.

> Longe de ser um fenômeno restrito a segurança ou letramento digital, o que os estudos indicam é que os criminosos têm explorado fatores situacionais ao identificar vítimas mais vulneráveis, diversificado os métodos de ataque e empregado técnicas de engenharia social (induzir usuários a enviar dados confidenciais) (Naidoo, 2020). (Anuário brasileiro de segurança pública, 2023, pág. 95).

O legislador expressa essas espécies de fraude considerando a recorrência dessas, mas possibilita uma interpretação analógica para acompanhar as inovações tecnológicas que possibilitam novos tipos de golpes. A internet, por exemplo, facilita transações bancárias e comerciais sem a necessidade de presença física do cliente, o que propiciou o surgimento de novas modalidades de fraude, muitas vezes difíceis de detectar e rastrear.

O legislador considerou essa dificuldade e, ao final do parágrafo, ampliou o escopo para incluir "qualquer outro meio fraudulento análogo", abrindo espaço para uma interpretação flexível e adaptativa. Essa previsão atende ao crescimento das fraudes eletrônicas que, graças ao avanço da tecnologia, estão em constante transformação, criando novas formas de enganar e ludibriar as pessoas (Nucci, 2023).

O estelionato digital segue a lógica do estelionato tradicional no que tange aos sujeitos do crime. O sujeito ativo pode ser qualquer pessoa que utilize ferramentas digitais para enganar, enquanto o sujeito passivo pode ser qualquer pessoa, física ou jurídica, que sofra prejuízo patrimonial em decorrência da fraude. O objeto

jurídico protegido, como no estelionato comum, é o patrimônio, sendo a sua preservação o foco central da norma (Nucci, 2023).

O objeto material do crime abrange uma diversidade de bens econômicos. No contexto das fraudes digitais, podem ser carteiras de investimento, ativos virtuais, valores mobiliários e outros ativos financeiros que, por meio de artifícios fraudulentos, são manipulados para garantir vantagem ilícita ao infrator. As criptomoedas, por exemplo, representam uma nova fronteira para os delitos patrimoniais, pois permitem transações anônimas e dificultam o rastreamento, características que tornam as fraudes ainda mais desafiadoras para o sistema penal. O Anuário Brasileiro de Segurança Pública destaca que essa preocupação é ainda crescente diante da tendência mundial de digitalização financeira:

> A preocupação pública com os crimes patrimoniais cometidos no ambiente digital ou a partir de meios eletrônicos tem crescido. A digitalização das finanças, de serviços e do comércio, especialmente impulsionada durante o período pandêmico, contribui com a formação de um ambiente propício ao desenvolvimento de modalidades criminais que exploram vulnerabilidades nestes segmentos (Anuário brasileiro de segurança pública, 2022, pág. 118).

O elemento subjetivo do crime é o dolo, ou seja, a intenção deliberada do agente de cometer a fraude com o objetivo de obter vantagem ilícita. Não há previsão de estelionato culposo, o que significa que o agente deve agir intencionalmente para prejudicar a vítima.

A Lei nº 13.964/2019 introduziu uma mudança importante, tornando a ação penal para crimes de estelionato condicionada à representação da vítima, exceto em casos específicos, como quando o sujeito passivo é a Administração Pública, menores de idade, pessoas com deficiência mental ou maiores de 70 anos. Embora a Lei nº 14.155, de 2021, tenha criado uma tipificação específica para fraudes eletrônicas no § 2º-A, a regra de ação penal pública condicionada à representação da vítima continua aplicável nesses casos. Isso garante que o sistema jurídico possa proteger adequadamente as vítimas, que podem ser especialmente vulneráveis em transações realizadas no ambiente digital.

A criação do § 2º-A do artigo 171 do Código Penal foi uma resposta à evolução das fraudes no ambiente virtual. A legislação brasileira se ajustou às novas realidades tecnológicas para assegurar que o patrimônio continue protegido em face das mudanças rápidas e constantes que ocorrem no mundo digital. A previsão de penas mais severas e a possibilidade de interpretar as fraudes de forma analógica refletem a urgência de enfrentar esses novos desafios e de garantir a segurança jurídica e patrimonial no contexto das inovações tecnológicas.

2.3 Fraudes eletrônicas utilizando inteligência artificial (IA)

A inteligência artificial (IA) é a área da ciência da computação que busca desenvolver sistemas capazes de realizar tarefas que normalmente exigiriam inteligência humana. Esses sistemas são programados para aprender, raciocinar, perceber e tomar decisões de forma autônoma, por meio de técnicas como aprendizado de máquina, redes neurais e processamento de linguagem natural. A IA já assumiu funções críticas em diversas áreas, como destaca Ana Luísa Simão:

> A inteligência artificial se faz presente em nosso dia a dia de diversas formas, tais como nos algoritmos de busca do Google, na recomendação de filmes do Netflix, no marketing digital, nos assistentes virtuais como Siri e Alexa, nas tecnologias de reconhecimento facial utilizadas pelo poder público e nas redes sociais (Direito, Tecnologia e Inovação, 2022, pág. 29).

Os crimes envolvendo IA cresceram rapidamente no cenário internacional nos últimos anos, à medida que criminosos passaram a usar essa tecnologia para cometer fraudes sofisticadas e em grande escala. Com a capacidade de processar grandes volumes de dados e criar interações personalizadas, a IA permite a execução de fraudes difíceis de serem detectadas por métodos tradicionais. Em vários países, fraudes eletrônicas como phishing e roubo de identidade têm se tornado mais difíceis de combater devido ao uso de IA para criar mensagens e interações cada vez mais convincentes. A tendência de crescimento das fraudes digitais e seu potencial perigo pode ser exemplificado na seguinte informação trazida pelo Anuário Brasileiro de Segurança Pública:

> O estelionato por meios tecnológicos gera tantos lucros para as organizações criminosas que até mesmo o Cartel de Jalisco Nova Geração, do México, criou estruturas de telemarketing que realizam golpes contra

> pessoas aposentadas nos Estados Unidos, sendo que o prejuízo de algumas vítimas chega a mais de um milhão de dólares, conforme destacado por reportagem do New York Times em março deste ano (Anuário brasileiro de segurança pública, 2024, pág. 102).

A Inteligência Artificial (IA) está emergindo como ferramenta para fraudes no Brasil, e o cenário é preocupante. A escalada massiva de tentativas de fraudes eletrônicas no país — principalmente via redes sociais, e-mails e aplicativos — revela uma vulnerabilidade crescente. A IA adiciona uma camada extra de sofisticação a essas fraudes, que já são numerosas, embora nem sempre convincentes. O uso da IA em larga escala permitirá que as fraudes, antes facilmente identificáveis, se tornem altamente personalizadas e, consequentemente, mais difíceis de detectar.

Esse cenário estende-se, inclusive, ao âmbito empresarial, uma vez que nem as empresas estão preparadas para lidar com essa transformação. Segundo o Anuário Brasileiro de Segurança Pública:

> Um estudo produzido pela Consultoria PwC intitulado “Índice Transformação Digital Brasil 2023”3 revela que apenas 3% das empresas e organizações consultadas pela equipe do projeto relataram iniciativas robustas associadas a práticas de cibersegurança, como análise preditiva de fraudes e reforço na segurança dos dados (Anuário brasileiro de segurança pública, 2024, pág. 100).

A capacidade da IA de personalizar fraudes em grande escala é uma das principais características que a tornam tão perigosa. A IA pode, por exemplo, coletar e analisar dados de centenas de milhares de vítimas ao mesmo tempo, personalizando as interações de maneira convincente para cada uma delas. Isso significa que, em vez de golpes genéricos, as vítimas recebem mensagens ou chamadas que parecem ter sido feitas sob medida para elas. Um exemplo disso é o uso de IA para analisar o comportamento online das vítimas e, em seguida, criar mensagens que pareçam vir de amigos ou familiares, aumentando a chance de a fraude ser bem-sucedida.

A IA possui outras características que a tornam ainda mais perigosa que as fraudes tradicionais. Uma dessas características é sua capacidade de automação, que permite que as fraudes sejam realizadas sem a intervenção humana, em uma

escala e velocidade sem precedentes. A IA pode operar 24 horas por dia, executando milhares de tentativas de fraude simultaneamente, com um nível de precisão que torna a detecção extremamente difícil. Outra característica é a sua habilidade de "aprender" e adaptar-se a diferentes contextos. Ao analisar os resultados das tentativas de fraude, a IA pode refinar suas táticas e melhorar sua eficácia ao longo do tempo.

O volume de fraudes eletrônicas já representa um desafio significativo para o Estado, mesmo que essas fraudes ainda sejam predominantemente manuais. O crescimento exponencial dessas práticas criminosas tem sobrecarregado as instituições de segurança pública. A introdução de inteligências artificiais capazes de gerar fraudes de forma automática e em larga escala, intensificará esse desafio. O Anuário Brasileiro de Segurança Pública destaca a dificuldade encontrada em lidar com o alto volume de fraudes:

> Embora no Brasil a tipificação de fraude eletrônica seja recente, o crescimento dos crimes de estelionato (que não diferencia aqueles em meio eletrônico dos demais) ocorreu de modo exponencial durante a pandemia de Covid-19, saltando de 426.799 ocorrências no ano de 2018 para 1.819.409 em 2022. Um crescimento da ordem de 300% desafia a lógica de trabalho de qualquer organização, que dirá das Polícias Civis brasileiras, que há anos vem sendo sucateadas e cujos efetivos estão reduzidos e envelhecidos. (Anuário brasileiro de segurança pública, 2023, pág. 96)

O Anuário Brasileiro de Segurança Pública de 2024 não apenas reconheceu essa tendência alarmante, mas também destacou especificamente a crescente utilização de "robôs" nessas fraudes. Essa menção explícita reflete a preocupação crescente das autoridades de segurança pública com a sofisticação tecnológica empregada pelos criminosos virtuais. A evolução das táticas fraudulentas, agora potencializadas pela automação e inteligência artificial, representa um novo paradigma na luta contra o crime cibernético, exigindo uma atualização constante das estratégias de prevenção e combate.

> “Além disso, as novas tecnologias permitem que os criminosos virtuais realizem os golpes em um volume muito maior, pois a partir de uma base de dados de telefones, por exemplo, podem criar robôs para enviar mensagens que busquem ludibriar literalmente milhões de vítimas em potencial. (Anuário brasileiro de segurança pública, 2024, pág. 101)”

As fraudes eletrônicas já são amplamente utilizadas por organizações criminosas, e sua associação com a IA potencializará significativamente os danos. Essa evolução tecnológica no mundo do crime organizado representa um salto qualitativo nas capacidades das organizações criminosas, potencializando seus ganhos ilícitos e ampliando sua esfera de influência no mundo digital. O Anuário Brasileiro de Segurança Pública de 2024 destaca a importância que as fraudes eletrônicas já têm no âmbito das grandes organizações criminosas brasileiras:

> No Brasil, há investigações que indicam que o Primeiro Comando da Capital (PCC) e o Comando Vermelho (CV) também criaram centrais para a práticas de golpes virtuais e por telefone, muitos deles com a utilização de meios de pagamento como o PIX e de contas 'laranjas' (Anuário brasileiro de segurança pública, 2024, pág. 102).

As fraudes eletrônicas já representavam um desafio significativo para as polícias devido à sua complexidade e especificidades, situação que se agravará com a introdução da inteligência artificial. O Anuário de Segurança Pública destaca como a adaptação às fraudes eletrônicas tem sido desafiadora, exigindo novas medidas. A utilização de IAs nas táticas criminosas cria uma disparidade crescente entre as capacidades dos criminosos e as habilidades das autoridades encarregadas de combatê-los. O desafio se apresenta da seguinte forma:

> Por fim, os autores chamam a atenção para a insuficiente formação dos policiais envolvidos nestas ocorrências, o que exige cursos altamente especializados e rotinas rígidas de atualização, dada a rapidez com que mudanças tecnológicas são introduzidas. Isto porque as habilidades necessárias aos profissionais envolvidos nas investigações de crimes eletrônicos são distintas daquelas comumente ensinadas nas academias de polícia para casos de homicídios ou roubos, e a natureza e rapidez da mudança tecnológica cria pressões para atualização deste conhecimento pelos profissionais de segurança (Anuário brasileiro de segurança pública, 2023, pág. 96).

Assim como foi necessário criar o § 2º-A no artigo 171 do Código Penal para enfrentar as fraudes eletrônicas, o alto risco trazido pela IA evidencia a necessidade de manter a legislação atualizada para evitar a proliferação desenfreada de fraudes assistidas por inteligência artificial no cenário brasileiro. É essencial compreender a estrutura penal brasileira para analisar se o § 2º-A do artigo 171 do Código Penal abrange as fraudes assistidas por IA e se essa previsão é suficiente.

3 DA ESTRUTURA PENAL BRASILEIRA

3.1 Tipicidade Formal e Material

Ao abordar a estrutura penal brasileira, é imperativo compreender o conceito fundamental e a divisão da conduta punível. Esta é caracterizada como uma ação que atende a três critérios essenciais: tipicidade, antijuridicidade e culpabilidade. Essa tríade constitui o cerne da teoria do crime no direito penal brasileiro, embora não seja a única doutrina existente, é certamente a mais proeminente e amplamente aceita entre os juristas e estudiosos do direito penal. O jurista Cezar Roberto Bitencourt destaca que essa divisão é francamente majoritária:

> O consenso francamente majoritário da doutrina no sentido de que a conduta punível pressupõe uma ação típica, antijurídica e culpável, além de eventuais requisitos específicos de punibilidade, é fruto da construção das categorias sistemáticas do delito — tipicidade, antijuridicidade e culpabilidade — (Bitencourt, 2020, p. 585).

A tipicidade refere-se à correspondência entre o ato praticado e a descrição formal contida na lei penal. A antijuridicidade, por sua vez, indica que a conduta é contrária ao ordenamento jurídico como um todo. Já a culpabilidade está relacionada à reprovabilidade da conduta do agente, considerando sua capacidade de entender o caráter ilícito do fato e de determinar-se de acordo com esse entendimento (Bitencourt, 2020).

Este trabalho tem como objetivo realizar uma análise sobre a possibilidade de enquadramento adequado das fraudes eletrônicas no tipo penal descrito no § 2º-A do artigo 171 do Código Penal brasileiro. Faz-se necessário, para esse fim, conduzir um exame da tipicidade, que constitui o primeiro elemento da teoria tripartida do crime.

Ao analisar o tipo penal no âmbito do direito, faz-se necessário compreender sua definição filosófica mais ampla e abrangente. O tipo, em sua essência, é tratado como um modelo conceitual ou um conjunto estruturado de circunstâncias que se aplicam a uma variedade de situações. Prado apresenta a seguinte definição filosófica do tipo:

> Em sede filosófica e geral – como modelo, forma ou esquema –, vem a ser o “conjunto coligado de características que pode ser repetido por um número indefinido de exemplares”. Ou, mais simplesmente, o conjunto de circunstâncias relevantes (Prado, 2019, pág. 857).

O conceito de tipo adquire contornos mais específicos quando inserido na realidade jurídica. O tipo, nesse caso, é apresentado como um construto teórico que se materializa em situações concretas do mundo jurídico. Prado descreve essa transição do conceito filosófico para o jurídico da seguinte maneira:

> “o tipo forma uma categoria mais concreta, singular e específica – com acentuado vínculo à realidade objetiva – presente nas ciências em geral e na ciência jurídica, em particular. Na ciência jurídica em geral, o tipo se apresenta basicamente como hipótese fática que deve ser objeto de valoração (Prado, 2019, pág. 858).

Essa transição da perspectiva filosófica para a jurídica permite que o tipo seja definido, no âmbito do direito, como o "conjunto dos elementos do fato punível descrito na lei penal". O tipo deve ser individual, e a conduta deve se amoldar perfeitamente a ele (Bitencourt, 2020).

A exigência de uma correspondência precisa entre a conduta e o tipo penal está intrinsecamente ligada ao princípio da legalidade, um dos pilares fundamentais do direito penal moderno. Este princípio estabelece uma relação simbiótica com o conceito de tipo penal, como elucidado por Prado:

> Com efeito, para que uma ação ou omissão constituam delito devem estar compreendidas num tipo de injusto do Código Penal ou de uma lei penal especial. Essa necessidade é derivada do princípio da legalidade, e implica função de garantia do tipo (princípio de tipicidade) (Prado, 2019, pág. 861)

O conceito de tipicidade emerge dessa análise do tipo penal. A tipicidade representa a correspondência entre o comportamento concreto do agente e a descrição abstrata contida na lei penal. Damásio de Jesus conceitua a tipicidade como “a correspondência entre o fato praticado pelo agente e a descrição de cada espécie de infração contida na lei penal incriminadora" (Jesus, 2014, pág. 228).

Essa compreensão da tipicidade faz necessária o surgimento do juízo de tipicidade que é um processo intelectual que consiste em uma análise minuciosa a fim de estabelecer se uma determinada conduta se enquadra nos parâmetros descritos pela lei penal. Bitencourt defende que:

> Há uma operação intelectual de conexão entre a infinita variedade de fatos possíveis da vida real e o modelo típico descrito na lei. Essa operação, que consiste em analisar se determinada conduta se adapta aos requisitos descritos na lei, para qualificá-la como infração penal, chama-se “juízo de tipicidade (Bitencourt, 2020, p. 770).

É através dessa adequação surge o conceito de tipicidade formal que é a adequação da conduta do agente ao modelo abstrato previsto na lei penal. Essa adequação deverá ser perfeita, a fim de considerar o fato formalmente típico (Greco, 2020).

Greco oferece um exemplo dessa adequação relacionando com o crime de furto, tipificado no art. 155 do Código Penal brasileiro. Ele explica que aquele que simplesmente subtrai coisa alheia móvel, não com o fim de tê-la para si ou para outrem, mas sim com a intenção de usá-la temporariamente, não comete o crime de furto. Isso ocorre porque no tipo penal em questão não existe a previsão específica dessa conduta, tornando, portanto, o chamado "furto de uso" uma ação não punível sob a égide do princípio da legalidade e da tipicidade formal (Greco, 2020).

Essa análise da tipicidade formal conduz à necessidade de abordar a tipicidade material, estabelecendo a distinção crucial entre esses dois conceitos. A tipicidade material, em contraposição à formal, pode ser compreendida da seguinte maneira:

> “É o tipo legal adequado à lesividade, que possa causar a bens jurídicos protegidos, bem como socialmente reprovável. Ex.: no caso das lesões corporais, somente se materializa a tipicidade material, caso haja o preenchimento dos elementos do art. 129, associados à efetiva lesão do bem jurídico tutelado, de maneira reprovável. Por isso, o furo na orelha de uma menina para a colocação de um brinco pode ser formalmente uma lesão à integridade corporal, mas, materialmente, trata-se de fato atípico, pois adequado socialmente (Nucci, 2023, 347).

Essa concepção de tipicidade material que torna possível e necessário excluir dos tipos penais aqueles fatos reconhecidos como de bagatela, ou seja, de mínima ofensividade, nos quais tem aplicação o princípio da insignificância. Esse critério da tipicidade material que afere e se avalia a real importância do bem jurídico no caso concreto, permitindo que os operadores do direito possam concluir se aquele bem específico merece ou não ser efetivamente protegido pela tutela do Direito Penal, considerando sempre o princípio da intervenção mínima e a função do direito penal como ultima ratio (Greco, 2020).

A distinção entre tipicidade formal e material é necessária no presente trabalho a fim de direcionar a compreensão para a adequação da conduta à tipicidade formal. Esta ênfase se justifica pelo fato de que a análise de interesse central neste estudo é determinar se as fraudes eletrônicas realizadas com o uso de inteligência artificial podem ser adequadamente enquadradas no § 2º-A do artigo 171 do Código Penal e, para isso, é fundamental considerar a forma como a legislação vigente realiza a análise da tipicidade formal.

3.2 Analogia vs. Interpretação Analógica

Nenhuma legislação, por mais abrangente e completa que seja, pode contemplar todas as situações que a complexidade da vida social apresenta ao longo do tempo. O direito possui uma natureza dinâmica e lacunosa, encontrando-se em constante transformação. Sendo parte integrante da sociedade, o direito evolui em conjunto com ela, recebendo continuamente a influência de novos fatos e circunstâncias. As normas jurídicas frequentemente se mostram insuficientes para regulamentar toda a diversidade de situações que a realidade social proporciona (Bitencourt, 2020).

Bitencourt destaca a natureza dinâmica e evolutiva do direito em face da complexidade social. Ele argumenta que:

> Nenhum sistema jurídico positivo é imune à presença de lacunas, especialmente um ramo fragmentário como é o Direito Penal. Como destacava Aníbal Bruno, “A vida, na sua evolução, se distancia do Direito legislado, ultrapassa-o e vai criar, assim, outras lacunas no sistema jurídico.

> Se novas leis não ocorrem para cobri-las, é ao juiz que cabe preenchê-las por meio do processo da analogia" (Bitencourt, 2020, pág. 445)

Essa característica gera necessidade de interpretação e integração das normas jurídicas. O processo interpretativo permite compreender o verdadeiro sentido e alcance das leis, enquanto a integração busca preencher as lacunas existentes no ordenamento jurídico.

Essas formas de interpretação e integração podem suscitar controvérsias no âmbito do Direito Penal. As principais problemáticas se concentram na interpretação extensiva, na interpretação analógica e na aplicação da analogia. Cada uma dessas abordagens deve ser diferenciada a fim de verificar a aplicável a análise pretendida pelo presente trabalho.

A interpretação extensiva é o processo meticuloso de extração do autêntico significado da norma, ampliando-se o alcance das palavras legais além de sua literalidade imediata, a fim de se atender à real finalidade do texto normativo, conforme idealizado pelo legislador (Nucci, 2023).

O autor Rogério Greco diferencia a interpretação extensiva como o gênero mais amplo, no qual se inserem como espécies a interpretação extensiva em sentido estrito e a interpretação analógica. Caso o legislador não tenha fornecido um padrão explícito a ser seguido e seja necessário ampliar o alcance do tipo penal para alcançar hipóteses não previstas expressamente, mas queridas por ele em sua intenção normativa, estaremos diante de uma interpretação extensiva em sentido estrito (Greco, 2020).

Essa distinção também é necessária entre a analogia e a interpretação analógica, dois conceitos relacionados, mas com aplicações distintas no âmbito jurídico. A analogia não é um método de interpretação da lei, mas um mecanismo de integração do sistema jurídico. Não há um texto legal que apresente obscuridade ou incerteza, mas a completa ausência de legislação específica para regular determinada situação fática. Trata-se de casos em que o legislador não previu expressamente uma norma para regular determinada circunstância. O aplicador do

direito precisa buscar em outras normas do ordenamento jurídico uma solução aplicável ao caso concreto, baseando-se na semelhança entre a situação não regulada e aquela prevista em lei (Bitencourt, 2020).

O conceito de analogia foi apresentado por Bitencourt através de uma citação de Bettiol, que a define como uma extensão de uma norma jurídica:

> A analogia, na verdade, como pontificava Bettiol, “consiste na extensão de uma norma jurídica de um caso previsto a um caso não previsto com fundamento na semelhança entre os dois casos, porque o princípio informador da norma que deve ser estendida abraça em si também o caso não expressamente nem implicitamente previsto” (Bitencourt, 2020, pág. 445).

Esse tipo de integração, embora necessária para preencher lacunas na lei, não é aplicável de forma irrestrita. Existem limites legais que restringem sua utilização, visando garantir a segurança jurídica e o princípio da legalidade. Ao tratar sobre as limitações, destaca-se a limitação no âmbito do direito penal, destacada por Bitencourt:

> O recurso à analogia não é ilimitado, sendo excluído das seguintes hipóteses: a) nas leis penais incriminadoras — como essas leis, de alguma forma, sempre restringem a liberdade do indivíduo, é inadmissível que o juiz acrescente outras limitações além daquelas previstas pelo legislador. Em matéria penal, repetindo, somente é admissível a analogia quando beneficia a defesa (Bitencourt, 2020, pág. 447).

Ao tratar da distinção entre a analogia e a interpretação analógica, Bitencourt defende que essas não se confundem, pois a interpretação analógica “decorre de determinação expressa da própria lei”. Essa diferença é abordada da seguinte forma pelo autor:

> Não se trata de analogia em sentido estrito, como processo integrativo da norma lacunosa, mas de “interpretação por analogia”, isto é, de um processo interpretativo analógico previamente determinado pela lei, ou seja, um meio indicado para integrar o preceito normativo dentro da própria norma, estendendo-o a situações análogas, como ocorre, por exemplo, no art. 71 do CP, quando determina “pelas condições de tempo, lugar, maneira de execução e outras semelhantes” (Bitencourt, 2020, pág. 449).

Caso o aplicador da lei, ao abranger situações não elencadas expressamente

no tipo penal, o legislador tenha fornecido uma fórmula casuística, detalhando exemplos específicos, seguindo-se a ela uma fórmula genérica que permite a expansão interpretativa, estaremos diante de uma situação que demanda uma interpretação analógica (Greco, 2020).

Essa fórmula casuística não é incomum na lei penal. O conteúdo da norma é completado através de uma aplicação analógica de casos semelhantes que se apresentem, por determinação da própria norma. Nucci exemplifica com o disposto no art. 121, § 2.º, III em que, “dadas as amostras pelo tipo, permite-se que o intérprete vá buscar outros meios similares aos primeiros, igualmente configuradores de insídia, crueldade ou perigo comum” (Nucci, 2023).

Esse artigo também é usado de exemplo por Greco que defende que:

> Quando o legislador fez inserir as expressões ou por outro meio insidioso ou cruel, ou de que possa resultar perigo comum, ele quis dizer que qualquer outro meio dissimulado ou que cause excessivo sofrimento à vítima e aquele que possa trazer uma situação de perigo a um número indeterminado de pessoas, embora não elencados expressamente por esse inciso, estão também por ele abrangidos e, em virtude disso, qualificam o crime de homicídio (Greco, 2020, pág. 120).

Esse exemplo evidencia a aceitação e incorporação pelo Código Penal da utilização da interpretação analógica. Esse método também encontra amplo respaldo tanto na doutrina jurídica quanto na jurisprudência. Cezar Roberto Bitencourt, assim como a corrente majoritária, que advoga em favor da aplicação da interpretação analogica e vedação da analogia no direito penal:

> Por isso, a interpretação analógica, ao contrário da analogia, pode ser, e normalmente é, aplicada às normas penais incriminadoras. Estas, em obediência ao princípio nullum crimen, nulla poena sine lege, não podem ter suas lacunas integradas ou colmatadas pela analogia, em obediência exatamente ao princípio nullum crimen sine praevia lege (Bitencourt, 2020, pág. 450).

Essa distinção faz-se necessária para a análise acerca da possibilidade das fraudes assistidas por inteligências artificiais serem enquadradas, através da interpretação analógica, no tipo penal descrito pelo § 2º-A do artigo 171 do Código Penal.

4 DA ANÁLISE DO ENQUADRAMENTO JURÍDICO

4.1 Análise da necessidade de atualização legislativa

A legislação brasileira deve estar atualizada a fim de enfrentar o desafio crescente das fraudes eletrônicas assistidas por Inteligência Artificial (IA) a fim de evitar uma expansão dessa prática delituosa. A introdução do § 2º-A no artigo 171 do Código Penal brasileiro demonstrou a capacidade do sistema legal de se adaptar às novas realidades criminais. O Anuário Brasileiro de Segurança Pública de 2022 apresenta dados sobre as fraudes eletrônicas no mesmo ano de promulgação da Lei Nº 14.155 DE 2021:

> Embora com limitações, como o fato de que 9 estados não terem informado os dados, neste primeiro levantamento foi possível identificar que, em 2021, foram registrados 60.590 casos de estelionato por fraude eletrônica (Anuário brasileiro de segurança pública, 2022, pág. 120).

Esta tipificação específica, mesmo que implementada após um período de crescimento significativo dos casos, emergiu como uma resposta direta à proliferação das fraudes digitais no cenário brasileiro. Essa medida legislativa destacou a necessidade de uma abordagem proativa frente às rápidas inovações tecnológicas. A relevância da atuação legislativa não se limita à mera criação de novos crimes. A tipificação do crime de estelionato em meio eletrônico revelou uma melhoria significativa na capacidade de monitoramento, tanto quantitativo quanto qualitativo, das fraudes digitais. O Anuário Brasileiro de Segurança Pública de 2022 enfatiza a importância desta abordagem específica:

> "A análise destes dados de forma associada fortalece a constatação de que o crescimento no número de registros de estelionato tem sido amplamente impulsionado pelas ocorrências em meio digital que, a partir de sua tipificação, poderão ser mais bem monitoradas pelas autoridades estaduais e pelo público geral nos próximos anos, assim como alvo de políticas públicas, a fim de enfrentar o problema que tem acometido cada vez mais a população brasileira (Anuário brasileiro de segurança pública, 2022, pág. 120).

O Anuário de 2024 traz à luz um aspecto importante desta evolução legislativa, destacando que os registros de fraudes eletrônicas, anteriormente à

tipificação específica, não ficavam necessariamente impunes, mas eram classificados sob outros tipos penais mais genéricos. A decisão legislativa de criar um tipo penal específico para estas ocorrências, mesmo já existindo enquadramentos possíveis em outras categorias, representou uma especificação importante no tratamento legal destas infrações. Essa tipificação ocorreu em 2021 e, mesmo não tendo sido de grande anterioridade, essa pequena vantagem temporal importou no combate eficiente. O fato de ganhar destaque no anuário brasileiro de segurança pública atual, em 2024, mesmo dois anos após sua promulgação, destaca a importância desta abordagem proativa e da tipificação relativamente rápida frente a um cenário criminal em constante mutação. A importância dessa tipificação é citada no seguinte trecho:

> Registros que antes eram classificados em outras naturezas delituosas passaram a ganhar uma categoria própria, trazendo à tona um fato que antes estava invisibilizado não obstante causar danos significativos para a sociedade brasileira (Anuário brasileiro de segurança pública, 2024, pág. 97).

Essa necessidade de tipificar o crime de estelionato em meio eletrônico apresenta-se atualmente em relação às fraudes através de IA. Isso ocorre pois, segundo o Anuário brasileiro de segurança pública de 2024, o Brasil enfrenta uma reconfiguração criminal em que tais crimes permanecem ganhando tração:

> Essa tendência é marcada pelo movimento de substituição dos roubos por modalidades como estelionatos, golpes virtuais e furtos e que, em 2023, não só se manteve como ganhou tração no país (Anuário brasileiro de segurança pública, 2024, pág. 96).

Essa preocupação com as fraudes assistidas por inteligência artificial é destaque no Anuário brasileiro de segurança pública de 2024 já com a preocupação de que os criminosos podem “criar robôs para enviar mensagens que busquem ludibriar literalmente milhões de vítimas em potencial. Esse é um desafio real que a segurança pública enfrenta atualmente e deve ser combatido de forma proativa pelo judiciário. (Anuário brasileiro de segurança pública, 2024).

A legislação específica contra fraudes eletrônicas foi essencial, mas sua implementação tardia limitou sua eficácia inicial. Isso ressalta a importância de uma

abordagem proativa na formulação de leis contra crimes tecnológicos aliada a um combate prévio a fim de combater a proliferação criminosa no início de seu desenvolvimento. Após três anos, a adaptação dos estados à nova legislação ainda é incompleta, revelando desafios na implementação uniforme. Alguns estados têm dificuldades em monitorar esses crimes eficientemente:

> No caso dos estelionatos por meio eletrônico, há uma dificuldade grande de se obter dados nacionais detalhados, já que muitas Unidades da Federação ainda não os contabilizam de forma separada do total de estelionatos, a exemplo de São Paulo (Anuário brasileiro de segurança pública, 2024, pág. 97).

Esses argumentos conduzem à conclusão de que é necessária uma atualização legislativa proativa, mesmo que a expressão "outro meio fraudulento análogo" possa, em teoria, englobar a utilização de IA. Uma tipificação específica para fraudes assistidas por inteligência artificial permitiria uma melhor compreensão e monitoramento desses crimes específicos. Essa legislação atualizada poderá abordar nuances específicas das fraudes por IA e combaterá de forma antecipada esse tipo de fraude eletrônica, respondendo rapidamente às evoluções tecnológicas no campo criminal.

4.2 Possível enquadramento da fraude com IA como meio fraudulento análogo

Ao abordar o enquadramento jurídico dos crimes cometidos com assistência de Inteligência Artificial (IA), é necessário considerar duas possibilidades distinta: primeiramente, as fraudes eletrônicas perpetradas no âmbito das redes sociais, dos contatos telefônicos ou do envio de correio eletrônico fraudulento; e, em segundo lugar, as fraudes eletrônicas cometidas por outros meio, mas com a assistência de inteligência artificial.

A primeira categoria se enquadra na parte inicial do artigo pertinente da legislação, sem necessidade de uma adequação analógica, mesmo quando há utilização de IA como ferramenta auxiliar na prática delituosa. Isto ocorre porque, após um juízo de tipicidade formal, verifica-se uma adequação típica perfeita ao texto da lei. A utilização de IA, nestes casos, não altera a natureza do crime nem sua classificação legal, sendo apenas um elemento que confere maior sofisticação à

execução do delito.

A segunda categoria exige uma análise sobre se a expressão "ou por qualquer outro meio fraudulento análogo", presente na legislação, é abrangente o suficiente para incluir os crimes cometidos com o uso de IA em contextos não explicitamente mencionados na lei. Essa questão pode ser abordada examinando situações similares no ordenamento jurídico brasileiro, onde se faz necessária uma interpretação analógica. Luiz Prado aponta diversas referências no Código Penal a condições semelhantes ou análogas, que demandam do intérprete da lei uma compreensão analógica do tipo. Ele cita os seguintes exemplos:

> Referência a condições semelhantes às de tempo, lugar, maneira de execução – art. 71, caput, CP (crime continuado); a outro recurso análogo à traição, emboscada, dissimulação – art. 61, II, c, CP (circunstâncias agravantes); às substâncias de efeitos análogos ao álcool – art. 28, II, CP (embriaguez); a outro sinal indicativo de linha divisória, como tapume ou marco – art. 161, CP (alteração de limites); ou a outro recurso – art. 121, § 2.º, IV, CP (homicídio qualificado). (Prado, 2019, pág. 385).

Essa análise requer, além dos exemplos já fornecidos, a apresentação do tipo penal em questão, que estabelece:

> Art. 171 - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento: Pena - reclusão, de um a cinco anos, e multa, de quinhentos mil réis a dez contos de réis. (Vide Lei nº 7.209, de 1984) (...) Fraude eletrônica § 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo (Incluído pela Lei nº 14.155, de 2021) (Código Penal, Artigo 171, § 2º-A).

Verifica-se que o artigo em tela apresenta características semelhantes aos demais tipos penais descritos por Regis Prado em sua obra. Essa semelhança é particularmente notável na maneira como o artigo delineia os elementos constitutivos do crime, bem como na gradação da pena conforme a gravidade e as circunstâncias específicas do delito.

A interpretação deste dispositivo legal deve ser realizada conforme o entendimento de Rógerio Greco. Ele argumenta que, quando o legislador apresenta

uma fórmula casuística, detalhando exemplos específicos, seguida de uma fórmula genérica que permite expansão interpretativa, estamos diante de uma situação que exige interpretação analógica (Greco, 2020). Esses exemplos específicos são “por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento” enquanto “por qualquer outro meio fraudulento análogo” é a fórmula genérica que permite expansão interpretativa.

Sobre o termo final "ou por qualquer outro meio fraudulento análogo", é pertinente considerar a perspectiva de Nucci, que defende que esta expressão já foi inserida pelo legislador prevendo futuros avanços tecnológicos. Nucci argumenta:

> Amplia-se ao final, prevendo qualquer outro mecanismo fraudulento análogo. Esta previsão, incluída pela Lei 14.155/2021, veio de encontro ao incremento das fraudes cometidas por diversos meios eletrônicos e informáticos, gerando novos e variados mecanismos capazes de armar ciladas para ludibriar as pessoas, cada vez mais levadas a esse cenário pelas inovações tecnológicas (Nucci, 2023, pág. 1269)

Esta interpretação de Nucci sugere que o legislador, ao incluir esse complemento, já antecipava a possibilidade de surgirem novas formas de fraude eletrônica e, ao incluir os termos “por qualquer outro meio fraudulento análogo”, já estaria tipificando novas formas de cometer tais fraudes eletrônicas, incluindo as cometidas com auxílio da inteligência artificial.

Esses argumentos conduzem à conclusão de que as fraudes eletrônicas assistidas por Inteligência Artificial (IA) estão contempladas no § 2º-A do artigo 171 do Código Penal. Esta interpretação se fundamenta em duas vertentes distintas: primeiramente, nos casos envolvendo redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, aplica-se uma adequação típica perfeita, independentemente do uso de IA como ferramenta auxiliar. A segunda hipótese, para as fraudes eletrônicas cometidas por outros meios, mas com assistência de IA, recorre-se a uma interpretação analógica da expressão "por qualquer outro meio fraudulento análogo".

5 CONSIDERAÇÕES FINAIS

O presente trabalho realizou uma análise da tipicidade das fraudes eletrônicas assistidas por inteligência artificial (IA) no contexto da Lei nº 14.155 de 2021. Esta investigação considerou não apenas a evolução histórica da tipificação do estelionato, mas também seu desenvolvimento até o cenário atual de avanço tecnológico atual, examinando a estrutura penal da legislação brasileira.Esse exame esclareceu as nuances entre analogia, interpretação analógica e interpretação extensiva e apontou a possibilidade de uma interpretação extensiva no § 2º-A do artigo 171.

Os desafios contemporâneos trazidos pelas IAs demonstraram a importância crucial de estabelecer um tipo penal específico. Esta especificidade é essencial para proporcionar um combate mais eficaz e um monitoramento mais preciso desse tipo de crime, de forma independente e complementar ao § 2º-A do artigo 171 do Código Penal . A criação de um tipo penal dedicado permitiria uma abordagem mais direcionada às rápidas mudanças associadas a esse tipo de tecnologia, associado a um combate e monitoramento de maior qualidade e eficiência.

A análise da aplicabilidade das fraudes eletrônicas assistidas por IA, realizada através de uma interpretação extensiva do termo "qualquer outro meio fraudulento análogo", revelou-se uma abordagem possível e amplamente aceita pela doutrina jurídica. Esta investigação também evidenciou as limitações inerentes a essa interpretação, destacando sua insuficiência para abordar completamente a complexidade e as particularidades das fraudes envolvendo IA. Esta constatação ressalta a necessidade de uma abordagem legislativa mais específica e abrangente.

Este estudo conclui que, embora seja tecnicamente possível enquadrar as fraudes eletrônicas assistidas por IA no âmbito do § 2º-A do artigo 171 do Código Penal através de uma interpretação extensiva, esta abordagem se mostra insuficiente para enfrentar plenamente os desafios apresentados por estas novas modalidades de crime. Para que o ordenamento penal brasileiro ofereça uma resposta verdadeiramente eficaz, justa e abrangente a essas fraudes tecnologicamente avançadas, faz-se necessário não apenas recorrer à interpretação analógica, mas também promover um aprimoramento legislativo substancial. Este aperfeiçoamento deve contemplar de forma específica e detalhada as

particularidades e nuances dessas condutas criminosas assistidas por IA. A implementação de uma legislação mais robusta e especializada nesta área não apenas fortaleceria significativamente o sistema penal no combate aos novos e complexos desafios impostos pela tecnologia, mas também asseguraria um maior rigor e precisão na aplicação da lei.

REFERÊNCIAS

Anuário Brasileiro de Segurança Pública / (2006)- . – São Paulo: FBSP, 2024. 404 p.: il

Fórum Brasileiro de Seguranç Pública. – 1 a

Anuário Brasileiro de Segurança Pública / (2006)- . – São Paulo: FBSP, 2023. 404 p.: il.

Fórum Brasileiro de Seguranç Pública. – 1 a

Anuário Brasileiro de Segurança Pública / (2006)- . – São Paulo: FBSP, 2022. 404 p.: il.

Fórum Brasileiro de Seguranç Pública. – 1 a

Anuário Brasileiro de Segurança Pública / (2006)- . – São Paulo: FBSP, 2021. 404 p.: il.

Fórum Brasileiro de Seguranç Pública. – 1 a

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidente da República, [2016]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 20 ago. 2024

BRASIL. Decreto-Lei 2.848, de 07 de dezembro de 1940. Código Penal. Diário Oficial da União, Rio de Janeiro, 31 dez.

BITENCOURT, Cezar Roberto *et al*. **Tratado de Direito Penal**. 26. ed. São Paulo: Saraiva, 2020.

ČERKA, Paulius; GRIGIENė, Jurgita; SIRBIKYTė, Gintarė. Liability for damages caused by artificial intelligence. **Computer Law & Security Review**, [S.L.], v. 31, n. 3, p. 376-389, jun. 2015. Elsevier BV.

CHESNEY, Robert; CITRON, Danielle. Deepfakes and the New Disinformation War: the coming age of post-truth geopolitics. **Foreing Affairs**, New York, p. 1-14, dez. 2018.

DOMINGOS, Pedro. The Master Algorithm: how the quest for the ultimate learning machine will remake our world. **Journal Of Computer Science And Technology.** La Plata, p. 1-3. nov. 2015.

ESTELLITA, Heloisa. **Responsabilidade penal de dirigentes de empresas por omissão**: estudo sobre a responsabilidade omissiva imprópria de diligentes de sociedades anônimas, limitadas e encarregados de cumprimento por crimes praticados por membros da empresa. São Paulo: Marcial Pons, 2017.

FLORIDI, Luciano *et al*. Ethics of Artificial Intelligence and Robotics. **Stanford Encyclopedia Of Philosophy.** Stanford, p. 1-30. abr. 2020.

GRACE, Katja *et al*. When Will AI Exceed Human Performance?: evidence from ai experts.
Journal Of Artificial Intelligence Research. Oxford, p. 729-754. jul. 2018.

GRECO, Rogério. **Curso de Direito Penal**: parte geral. 17. ed. Niterói: Impetus, 2020.

JANUÁRIO, Túlio Felippe Xavier. Inteligência Artificial e Responsabilidade Penal no Setor da Medicina. **Revista Portuguesa de Direito**, Coimbra, v. 17, n. 34, p. 1-27, dez. 2020.

LLINARES, Fernando Miró. INTELIGENCIA ARTIFICIAL Y JUSTICIA PENAL: más allá
de los resultados lesivos causados por robots. **Revista de Derecho Penal y Criminología**, [S.L.], n. 20, p. 87-130, 23 jan. 2020. UNED - Universidad Nacional de Educacion a Distancia.

MITTELSTADT, Brent. Principles alone cannot guarantee ethical AI. **Nature Machine Intelligence**, [S.L.], v. 1, n. 11, p. 501-507, 4 nov. 2019. Springer Science and Business Media LLC.

NUCCI, Guilherme de Souza. **Manual de direito penal**. 16. ed. São Paulo: Revista dos Tribunais, 2020. 1134 p.

OLIVEIRA, Ruy Flávio de. **Inteligência Artificial**. Londrina: Editora e Distribuidora Educacional S.A, 2018. 224 p.

OUSSEINI, Mounkaila Boutchi. Artificial Intelligence and Ethics: why responsible ai requires a critical approach.. **Ai & Society**, [*s. l*], 2018.

PAGALLO, Ugo. The Laws of Robots. **Law, Governance And Technology Series**, [S.L.],
v. 1, n. 1, jan. 2013. Springer Netherlands.

PRADO, Luis Regis. **Curso de Direito Penal**: parte geral. 5. ed. São Paulo: Revista dos Tribunais, 2019. 1508 p.

PRADO, Luis Regis. **Tratado de Direito Penal Brasileiro**. 3. ed. Rio de Janeiro: Forense, 2019.

RODRIGUES, Ana Paula da Fonseca; SILVA, Roberto Ferreira Archanjo da; POUSADA, Estevan Lo Ré. INTELIGÊNCIA ARTIFICIAL, LESÃO A BENS JURIDICOS PENAIS E
RESPONSABILIDADE PENAL. **Relações Internacionais no Mundo Atual**, Curitiba, v. 2,
n. 35, p. 239-253, 2022.

SIMÃO, Ana Luisa Teotônio Josafá *et al*. **Direito, tecnologia e inovação**. Belo Horizonte: Dti Br, 2022. 450 p.

ZARSKY, Tal. The Trouble with Algorithmic Decisions. **Science, Technology, & Human Values**, [S.L.], v. 41, n. 1, p. 118-132, 14 out. 2015. SAGE Publications.