RESPONSABILIDADE PENAL NOS CRIMES COM USO DE INTELIGÊNCIA ARTIFICIAL

CRIMINAL LIABILITY FOR CRIMES COMMITTED WITH THE USE OF ARTIFICIAL INTELLIGENCE

Cassio Amauri Silva[1], Matheus Alexandre Rodrigues[2], Luis Carlos Simionato Junior[3]

[1] Acadêmico do Curso de Bacharelado em Direito das Faculdades Integradas dos Campos Gerais – CESCAGE.
[2] Acadêmico do Curso de Bacharelado em Direito das Faculdades Integradas dos Campos Gerais – CESCAGE.
[3] Doutor em Ciências Jurídicas Criminais e docente do Curso de Bacharelado em Direito das Faculdades Integradas Campos Gerais – CESCAGE.

Resumo: Este trabalho, busca analisar a responsabilidade penal nos crimes cometidos com o uso de Inteligência artificial, por meio das leis brasileiras vigentes, e projetos de lei que visam regulamentar o desenvolvimento e uso dessa tecnologia. Trata-se de uma pesquisa qualitativa, sendo o método dedutivo, com técnicas de pesquisa documental e bibliográfica. Assim, o artigo foi estruturado em 7 capítulos, onde é feita uma introdução de leis que abordam o uso da internet no Brasil. Em seguida, se apresenta os tipos de Inteligências Artificiais e principais crimes cometidos com o seu auxilio. Por fim a responsabilidade penal nos crimes cometidos com o uso de Inteligências Artificiais. Apontando ao final a necessidade da regulamentação e a tipificação própria dos crimes cometidos com o uso de Inteligência Artificial.

Palavras chave: Responsabilidade penal; Inteligência Artificial; Legislação Brasileira.

Abstract: The following scientific article seeks to analyze criminal liability in crimes committed with the use of Artificial Intelligence, through current Brazilian laws, and bills that aim to regulate the development and use of this technology. This is qualitative research, with a deductive method, using documentary and bibliographic research techniques. Thus, the article was structured into 7 chapters, which introduces laws that address the use of the internet in Brazil. Next, the types of Artificial Intelligence and the main crimes committed with their help are presented. Finally, criminal liability for crimes committed with the use of Artificial Intelligence. Finally, pointing out the need for regulation and the specific classification of crimes committed with the use of Artificial Intelligence.

Keywords: Criminal liability; Artificial intelligence; Brazilian Legislation.

Contato: matheus-ar94@hotmail.com; luis.junior@cescage.edu.br; cassio.silva0996@aluno.cescage.edu.br

INTRODUÇÃO

Este artigo tem como objetivo, analisar a possibilidade de responsabilidade penal nos crimes cometidos com o uso de Inteligência Artificial. No mundo contemporâneo, o surgimento

de novas tecnologias é constante, aparecendo em diversas áreas da sociedade, que vai desde tecnologias para facilitar as tarefas do cotidiano, até mesmo para entretenimento e lazer.

Ocorre que na medida que surgem novas tecnologias, as quais acabam por influenciar e alterar o cotidiano das pessoas, acabam por surgir novos delitos que venham a causar danos a outrem.

Um exemplo de crime cometido com o auxílio de Inteligência artificial, é o chamado "deepfake", onde criminosos, acabam editando, ou até mesmo criando, imagens, áudios e vídeos, colocando as vítimas em situações falsas, as quais acabam por atacar a imagem e honra dessas pessoas.

Mas a indagação que surge é, como está sendo tratado o assunto de crimes cometidos no âmbito da internet, e como punir os agentes que cometem tal delito.

> Sempre foi um desafio tratar de crimes informáticos com um Código Penal da era do Rádio. Nosso Decreto-Lei n. 2.848/40, embora tutele a maioria dos delitos informáticos, é omisso em questões onde a informática deveria ser o bem protegido pelo Direito Penal (Jesus; Milagre, 2016, p.33,).

No Brasil, até o ano de 2014, não se tinha nenhuma lei que regulamentasse o uso e desenvolvimento da internet em território nacional, e uma norma referente a crimes de informática surgiu somente em 2012, após o caso da atriz Carolina Dieckmann, onde teve seu computador invadido, e foram furtadas fotos intimas, as quais foram divulgadas na internet pelo autor do delito.

O fato de não possuir normas que preveem a responsabilidade penal em crimes usando Inteligências Artificiais, e a internet, geram, além de uma insegurança jurídica, mas também a sensação de impunidade, uma vez que, não tendo uma legislação especifica, o magistrado precisa utilizar de leis anteriores ao surgimento da internet.

Assim, o presente trabalho tem como objetivo geral, apresentar como a legislação brasileira tem regulado o uso de Inteligência Artificial, analisando as legislações vigentes, e um breve panorama para o futuro, através dos projetos de lei em tramitação.

Como objetivo especifico, se tem o estudo sobre a responsabilidade penal do agente que comete crimes com o uso de Inteligências Artificiais, discutindo sobre a necessidade de leis especificas para a tipificação dos crimes cometidos na internet.

Utiliza-se o Método Dedutivo, partindo da norma geral de responsabilidade penal nos crimes cometidos na internet, até casos específicos. Quanto as técnicas utilizadas, tem-se a técnica de pesquisa documental e a técnica de pesquisa bibliográfica. Sendo a técnica de

pesquisa documental voltada para a análise de fontes primárias como a lei e a jurisprudência e a técnica de pesquisa bibliográfica voltada para as fontes secundárias: doutrina e trabalhos científicos.

Para abordar o tema, o presente artigo foi dividido em 7 capítulos, onde é feita uma breve introdução de legislações que regulam o uso de internet, no segundo é abordado sobre os tipos de Inteligências Artificiais, em seguida se estuda sobre as IA no ordenamento jurídico brasileiro e estrangeiro. Analisa os principais crimes cometidos com o uso de Inteligência Artificial, e por fim trata-se da responsabilidade penal nos delitos com o uso de Inteligência Artificial.

1. LEGISLAÇÕES QUE ABORDAM O USO DA INTERNET NO BRASIL

Neste capitulo, antes de abordar o assunto das Inteligências Artificiais, se faz necessário abordar o tema desde o início comercial da internet no Brasil em 1995, e como o judiciário e o legislativo vem trabalhando para a sua regularização, e possíveis sanções cíveis e penais, em caso de delitos cometidos na internet ou com o uso dela.

1.1 Marco Civil da Internet (LEI 12.965/2014)

A difusão da internet no Brasil, após ter seu comercio iniciado em 1995 (Arruda, 2011), facilitou os brasileiros as possibilidades que o mundo on-line tem para oferecer. Como consequência, se teve um grande avanço tecnológicos, com o surgimento de ferramentas, softwares, redes sociais, moedas digitais e mais recentemente as Inteligências Artificiais.

Em abril de 2014 entrou em vigor no Brasil, a lei 12.965, também conhecida como Marco Civil da Internet, sendo a primeira lei brasileira, que em seu texto buscou regulamentar o desenvolvimento da internet em todo território nacional, bem como os direitos e deveres dos internautas (Brasil, 2014).

O Marco Civil da Internet se propõe como a resposta legislativa para regulamentar essas relações e trazer segurança jurídica. Sobre o Marco Civil da Internet, Teffé (2015, p. 4-5), faz um resumo do conteúdo do Marco Cível da Internet:

> Ao longo de 32 artigos, o Marco Civil da Internet estabelece direitos e deveres para o uso da Internet, além de regular temas específicos como a proteção aos registros, aos dados pessoais e às comunicações privadas, a neutralidade da rede, a responsabilidade civil dos provedores de conexão e aplicações de internet, a guarda de registros e a sua eventual requisição pelas autoridades. Da leitura, percebe-se a importância conferida aos princípios da neutralidade da

> rede, da privacidade e, principalmente, da liberdade de expressão, que preconiza a necessidade de se garantir um discurso livre e plural na rede que não sofra uma indevida interferência externa ou uma eventual censura prévia.

Entre os principais pontos abordados por esse dispositivo, se tem o capitulo dois, o qual traz em seu texto os direitos e garantias dos usuários de internet no Brasil, reforçando os direitos fundamentais previstos na Constituição Federal de 1988, como a inviolabilidade da intimidade e da vida privada, a inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial.

Outro destaque, é a responsabilidade de danos decorrentes de conteúdos gerados por terceiros, onde os não podem ser responsabilizados com conteúdo publicado por terceiros, conforme artigo 18 desta lei, "O provedor de conexão à internet não será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros", (Brasil, 2014).

Queiroz (2018) esclarece que a regra de responsabilização civil impõe a responsabilidade por fato próprio, só respondendo quem causa a conduta. Assim, "o próprio autor da postagem ofensiva – em geral, pessoas físicas – responderá pelo ilícito causado". Razão pela qual, a responsabilidade por atos de terceiros, são exceção.

Salvo em casos em que, após decisão judicial, não tomar as previdências necessárias, no âmbito dos seus limites técnicos. Conforme o artigo 19 desta lei:

> Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário (Brasil, 2014).

Basicamente, o Marco Civil da Internet, apesar de em seu texto busca garantia de direitos constitucionais fundamentais no uso da rede mundial de computadores, menciona sobre reparação civil dos danos causados com o uso da internet no Brasil, porém sem abordar a responsabilidade penal de usuários, bem como de provedores de internet.

1.2 Lei dos crimes cibernéticos (LEI 12.737/2012)

A lei dos crimes cibernéticos, também apelidada de lei Carolina Dieckmann, em referência ao caso, em que a atriz teve seu computador invadido, onde foram furtadas 36 fotos, e após sofrer uma tentativa de extorsão, as fotos intimas foram divulgadas na internet (Araújo, 2023).

Criada no ano 2012, a lei dos crimes cibernéticos traz alterações relevantes, dentre eles, o reconhecimento e inclusão de novos tipos penais, sendo a conduta do artigo 154-A e o

artigo 154-B, ambos do Código Penal Brasileiro.

Tal dispositivo legal tem como finalidade a descrição, para que assim seja tipificada como uma conduta ilícita a invasão de computadores e similares, conforme descrito em seu texto:

> Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita (Brasil, 2012).

Foi a primeira lei no Brasil a tratar de crimes na internet e descrevendo condutas que antes apenas eram repreendidas pela sociedade, e agora constituem um tipo penal incluso no Código Penal.

Doutrinadores classificam a lei 12.737/2012, bem como a conduta tipificada, "invasão de dispositivo informático, representa um crime de perigo abstrato, onde não se espera a ocorrência de resultado, forma legislativa que cresce diante do avanço da tecnologia e o temor do risco do seu uso indevido" (Jesus; Milagre, 2016, p.15).

A Lei 12.737/2012 incluiu no Código Penal regras para interrupção ou perturbação de serviço informático, telemático ou de informação de utilidade pública e ainda a equiparação de cartão de crédito ou débito a documento particular (Brasil, 2012), com isso, trazendo uma maior segurança jurídica, pois ao tipificar de maneira especifica as condutas de crimes de informática, tanto a acusação quanto a defesa, conseguem desempenhar seu trabalho, amparado por um dispositivo próprio, não precisando usar de analogia para o oferecimento de denúncia.

1.3 Lei de Fraudes Eletrônicas (Lei 14.155/2021)

Em 28 de maio de 2021 entrou em vigor a lei 14.155, a qual trouxe modificações ao Código Penal Brasileiro, em crimes cometidos na internet ou com dispositivos eletrônicos, principalmente nos crimes de furto e estelionato.

Com relação ao crime de furto, no artigo 155, parágrafo 4º-B do Código Penal, é uma qualificadora do delito de furto.

> § 4º-B. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo (Brasil, 2021).

Interessante reparar que o legislador, além de expressamente dispensar a existência de mecanismo de segurança, anota uma cláusula de abertura "ou qualquer outro meio fraudulento análogo". Ou seja, caso surjam outros meios análogos ao dispositivo eletrônico ou informático,

a conduta seguirá sendo punida criminalmente.

2. TIPOS DE INTELIGÊNCIAS ARTIFICIAIS

Após o início da comercialização da internet, se teve um grande avanço no desenvolvimento de novas tecnologias, com isso surgiram novas ferramentas e softwares, os quais auxiliam para a realização de atividades cotidianas, ou mesmo para lazer. Sendo uma das ferramentas que evoluiu em um pequeno espaço de tempo, foram as Inteligências Artificiais.

Atualmente existem várias inteligências artificiais, que vão desde os algoritmos de redes sociais, serviços de streaming, onde através de dados coletados, fazem a indicação de novos filmes series, chegando até a inteligências artificiais que emulam o pensamento humano. A classificação das Inteligências Artificiais, é realizada de acordo com sua capacidade e funcionalidade, existindo assim três tipos principais de IA.

Inteligência Artificial Limitada, conhecida também como Inteligência Artificial Fraca, não são capazes de raciocinar sozinhas, porém conseguem armazenar uma grande quantidade de dados, e através desses dados desempenham as funções para qual foram programadas. Existindo uma subcategoria de Inteligência Artificial, sendo as maquinas reativas e memória limitada. (Salesforce Brasil,2024).

As maquinas reativas, são Inteligências Artificiais que armazenam dados, e reagem a comandos para quais foram programados.

> O modelo mais antigo, básico e simples. Elas foram projetadas para reconhecer padrões e tomar decisões com base em dados presentes no momento, sem considerar informações passadas. Em outras palavras, esse tipo de máquina não tem memória ou capacidade de aprendizado (Andrade, 2024).

Se tem o seguinte conceito para as Inteligências Artificiais de memória limitada.

> A memória limitada é um tipo de inteligência artificial capaz de aprender com base em dados históricos. A partir dessas informações, ela consegue realizar tarefas específicas de forma autônoma – por isso não consegue aplicar seu conhecimento em áreas diferentes (Andrade, 2024).

O segundo tipo é a Inteligência Artificial Geral, também chamada de IA Forte, sendo essas capazes de executar tarefas similares as dos seres humanos, tendo a capacidade de aprender, através de técnicas chamada *machine learning.*

> Machine learning é o uso de algoritmos para organizar dados, reconhecer padrões e fazer com que computadores aprendam com esses modelos para gerar insights inteligentes sem a necessidade de pré-programação [...] os algoritmos de machine learning aprendem a partir dos dados inseridos em si. Assim, as máquinas são treinadas para aprender a executar diferentes tarefas

de forma autônoma (Salesforce Brasil, 2024).

E por fim a Superinteligência Artificial, a qual atualmente só existe no campo teórico, onde se discute se ela terá inteligência superior ao dos seres humanos em algumas áreas, devido a sua grande capacidade de armazenar e processar dados, além de ser capaz de raciocinar e tomar decisões sozinhas, além do que fora programada (Salesforce Brasil, 2024).

3. A INTELIGÊNCIA ARTIFICIAL NO ORDENAMENTO JURÍDICO BRASILEIRO

Por se tratar de um ramo novo no direito, o ordenamento jurídico brasileiro, não possui uma regulamentação de desenvolvimento, comercialização e consequentemente a responsabilidade penal.

A primeira proposta para regulamentação foi o Projeto de Lei 21 de 2020 (Câmara dos Deputados, 2020), que se encontra em tramitação no Congresso Nacional, busca estabelecer fundamentos e princípios para o desenvolvimento e aplicação das IA no Brasil, bem como sua definição de Inteligência Artificial:

> Art. 2º Para os fins desta Lei, considera-se sistema de inteligência artificial o sistema baseado em processo computacional que, a partir de um conjunto de objetivos definidos por humanos, pode, por meio do processamento de dados e de informações, aprender a perceber e a interpretar o ambiente externo, bem como a interagir com ele, fazendo predições, recomendações, classificações ou decisões, e que utiliza, sem a elas se limitar, técnicas como:
>
> I – sistemas de aprendizagem de máquina (machine learning), incluída aprendizagem supervisionada, não supervisionada e por reforço;
>
> II – sistemas baseados em conhecimento ou em lógica; III – abordagens estatísticas, inferência bayesiana, métodos de pesquisa e de otimização.
>
> Parágrafo único. Esta Lei não se aplica aos processos de automação exclusivamente orientados por parâmetros predefinidos de programação que não incluam a capacidade do sistema de aprender a perceber e a interpretar o ambiente externo, bem como a interagir com ele, a partir das ações e das informações recebidas (Brasil, 2024).

Outro projeto de lei tramitando no Senado Federal é a PL 2.338/2023, onde além de regulamentar o desenvolvimento das Inteligências Artificiais, já começou a discutir sobre a responsabilidade penal e civil, conforme os artigos 18 e 19, da primeira emenda feita sobre esse projeto de lei.

> Art. 18º. A responsabilidade por danos, civis ou penais, decorrentes da utilização de sistemas de IA classificados como de Baixo Risco é imputada exclusivamente ao operador ou usuário de sistema de IA que deliberadamente empregou o referido sistema.
>
> Art. 19º. A responsabilidade por danos, civis ou penais, decorrentes da utilização de sistemas de IA classificados como de Médio Risco recai sobre o desenvolvedor do sistema quando tais danos forem resultado de decisões autônomas tomadas pelo sistema (Brasil, 2023).

O projeto de lei 2.338, já teve 148 emendas, o que demonstra a importância da regulamentação do desenvolvimento e uso das Inteligências Artificiais no Brasil, pois o uso indevido dessas tecnologias, sem a devida regulamentação, poderá causar inúmeros danos, consequentemente a ações judiciais, com a insegurança de não ter previsão legal para responsabilizar o autor do ato ilícito.

4. LEGISLAÇÕES ESTRANGEIRAS SOBRE INTELIGÊNCIA ARTIFICIAL

O Brasil não é o único país que está em processo legislativo para a regulamentação do desenvolvimento e uso das Inteligências Artificiais, bem como a responsabilidade penal dos delitos cometidos com o uso dessa tecnologia.

A Comissão Europeia, em 2021 o *Artificial Intelligence Act.* (AI Act), sendo uma proposta de regulamentação e harmonização das regras sobre Inteligências Artificiais, sendo seus objetivos específicos:

> garantir que os sistemas de IA colocados no mercado da União e utilizados sejam seguros e respeitem a legislação em vigor em matéria de direitos fundamentais e valores da União, garantir a segurança jurídica para facilitar os investimentos e a inovação no domínio da IA, melhorar a governação e a aplicação efetiva da legislação em vigor em matéria de direitos fundamentais e dos requisitos de segurança aplicáveis aos sistemas de IA, facilitar o desenvolvimento de um mercado único para as aplicações de IA legítimas, seguras e de confiança e evitar a fragmentação do mercado (Comissão Europeia, 2021).

Nos Estados Unidos, no ano de 2022, foi apresentado pela Casa Branca o chamado *blueprint for an ai bill of rights*, trata-se de um documento, sendo mais uma recomendação política, ou seja, não possui caráter normativo, mas sim como um documento para auxiliar a criação de políticas e valores nas Inteligências Artificiais (Castro; Marques; Kauffman, 2024).

Outro país a criar regras para o uso de Inteligências Artificiais foi a China, principalmente referente a IA Generativa, que é a capaz de criar imagens, áudios e vídeos.

> A China é pioneira em várias leis na área de IA, como a Lei de Proteção de Informações Pessoais, a Lei de Segurança de Dados e as Disposições Administrativas sobre Algoritmos de Recomendação em Serviço de Informação Baseados na Internet, dentre outras. Com a ambição de se tornar líder global em IA até 2030, o país vem realizando esforços significativos para impulsionar esta tecnologia (Rivelli; Silveira, 2023).

Em uma análise sobre como a Inteligência Artificial está sendo regulamentada, se tem em comum um órgão regulamentador, que dita as diretrizes e funcionamento do desenvolvimento das IAs, bem como fica responsável pela questão de infrações cometidas com o uso dessa tecnologia.

Sendo assim, demais países estão preocupados com a regulamentação das Inteligências Artificiais, tanto no seu desenvolvimento, mas também para a responsabilidade cível e penal em ilícitos cometidos com o uso dessas tecnologias.

5. CRIMES FACILITADOS COM O USO DE INTELIGÊNCIAS ARTIFICIAIS

O uso da internet e das tecnologias de Inteligência Artificial (IA) tornou-se parte integrante do cotidiano de uma parcela significativa da população mundial. Por meio de redes sociais, plataformas de entretenimento e diversos serviços digitais, a conectividade e a automação se transformam a maneira como as pessoas interagem, se informam e realizam tarefas cotidianas. Essa revolução tecnológica não apenas facilitou a comunicação e o acesso à informação, mas também gerou novos desafios, entre eles a prevenção de cometimento de crimes na internet com o uso de IA.

> Com a expansão do uso dos computadores e com a difusão da Internet, tem-se notado, ultimamente, que o homem está se utilizando dessas facilidades para cometer atos ilícitos, potencializando, cada vez mais, esses abusos cometidos na rede. Como todos os recursos à disponibilidade do ser humano, a Informática e a telecomunicação não são usadas apenas para agregar valor. O abuso (desvalor) cometido por via ou com assistência dos meios eletrônicos não tem fronteiras (Rosa, 2006, p. 46).

Atualmente, diversos crimes são crimes na internet, tornando-se cada vez mais detalhados às vítimas e mais difíceis de serem evitados, à medida que as ameaças aprimoram suas estratégias para aplicar golpes e fraudes, aliado ao uso de Inteligências Artificiais, a chance de uma vítima cair aumenta significativamente.

Os principais crimes cometidos com o uso de Inteligência Artificial são:

Se tem o *Phishing*, onde os criminosos tentam obter informações pessoais, como senhas, número de cartão de crédito, se fazendo passar por empresas confiáveis.

> O *phishing scam* (pescaria de senhas), técnica, consiste em apenas uma das formas para que o agente obtenha vantagem ilícita, induzindo alguém em erro (conduta) e proporcionando a entrega ao atacante de informações confidenciais da vítima (Jesus; Milagre, p.18, 2016).

Com o uso de Inteligência Artificial, o *phising* acaba se tornando mais sofisticado, fazendo com que fique mais fácil para os criminosos a obtenção de dados pessoais, principalmente relacionado a cartão de crédito e conta bancária.

> A IA pode ser usada para gerar e-mails de *phishing* altamente persuasivos, que se assemelham a comunicações legítimas. Além disso, algoritmos de IA podem se adaptar com o tempo, tornando os ataques de *phishing* mais difíceis de serem detectados (Homework, 2023).

Fraude financeira: a IA pode ser usada para analisar grandes quantidades de dados financeiros e identificar padrões usados por grandes empresas, e usar essas informações para atividades fraudulentas, como lavagem de dinheiro, manipulação de mercado ou roubo de identidade.

> A capacidade da IA de aprender, adaptar-se e executar tarefas com eficiência sobre-humana torna-a uma ferramenta valiosa para os fraudadores, que buscam explorar vulnerabilidades do sistema financeiro, de plataformas de e-commerce e do setor industrial (Aras, 2024).

Fraude online: os criminosos podem usar inteligência artificial para criar perfis falsos em redes sociais, criar conteúdo falso, gerar comentários automatizados em fóruns e sites de avaliação, manipular algoritmos de recomendação e enganar os usuários para que façam compras fraudulentas ou cliquem em links maliciosos.

Outro crime que vem se tornando cada vez mais comum, o qual possui um grande potencial de causar inúmeros danos a vítima, é a manipulação de vídeos, áudios e imagens, conhecida como *deepfake,* que será melhor abordado no próximo capitulo, onde os criminosos usam Inteligências Artificiais para editar fotos e vídeos, fazendo-os parecer autênticos, para uso de chantagem, difamação, desinformação e manipulação política.

6. DEEPFAKES

Dentre as tecnologias que mais tiveram avanços nos últimos anos, foram as Inteligências Artificiais, onde algumas são capazes de editar vídeos e fotos. Ao usar apenas uma foto e poucos segundos de um áudio com a voz de uma pessoa, é possível criar um vídeo totalmente novo, de uma situação ou frase nunca dita pela pessoa.

Aliado ao fato de mais de 140 milhões de brasileiros possuírem contas em redes sociais, criminosos estão cometendo o chamado *deepfake*, onde eles manipulam vídeos e fotos, e postam nas redes sociais, com a finalidade de ferir a honra da vítima.

Sendo mais comum, e com maior visibilidade, são os *deepfakes* cometidos contra famosos, onde são criados vídeos e fotos com cunho sexual, e são divulgados através das redes sociais, que são republicados e compartilhados em massa.

Caso mais recente de enorme repercussão, envolvendo o crime de *deepfake,* foi o da cantora norte-americana Taylor Swift, onde usaram de Inteligência Artificial, para criar imagens de conteúdo pornográfico, fazendo parecer que era a própria Taylor, nas imagens. As imagens falsas de Taylor Swift foram divulgadas no Telegram e no X (antigo Twitter). As redes

sociais agiram para remover o conteúdo, e o X chegou a impedir que o nome da cantora fosse pesquisado por algumas horas. Entretanto, tais medidas não foram capazes de evitar que a postagem tivesse 45 milhões de visualizações e mais de 24 mil compartilhamentos. (Migalhas,2024).

Diversas celebridades e famosos brasileiros também foram afetados pelo uso de Inteligência Artificial para incluir seus rostos e vozes em diversos vídeos.

> Pedro Bial, William Bonner, Drauzio Varella, Cesar Tralli e Anitta estão tendo suas imagens veiculadas em vídeos que utilizam a tecnologia deep fake para clonar vozes e rostos para promover produtos de qualidade duvidosa, como remédios para calvície e jogos de azar (Miyashiro, 2024).

Ocorre que tal delito tem se tornado cada vez mais comum no nosso cotidiano, onde plataformas de vídeos curtos, e as redes sociais, ajudam a propagar os conteúdos adulterados pelos criminosos, fazendo com que se faça necessário a regulamentação, e a previsão de responsabilização penal, a fim de evitar a impunibilidade do agente que comete o delito, bem como, ao ser regulamentada uma punição, pessoas deixarão de praticar tal conduta.

6.1. Projeto de Lei sobre *deepfake* contra mulheres

No ano de 2023, foi apresentado o projeto de lei 5.695 (Câmara de Deputados, 2023), com a proposta de tipificação penal para quem altera fotos, vídeos e sons, para praticar crimes de violência contra mulher com o Uso de Inteligência Artificial, conforme a redação do projeto:

> Alterar manipular ou adulterar fotos, vídeos ou sons, utilizando-se de sistema de inteligência artificial, com o intuito de causar constrangimento, humilhação, assédio, ameaça ou qualquer outro tipo de violência à mulher, no âmbito doméstico ou familiar.
> Pena reclusão, de um a dois anos, e multa (Brasil,2023).

No projeto em questão se busca a regulamentação e responsabilização penal para quem busca praticar crimes com o uso de IA no âmbito da Lei Maria da Penha, apesar de se tratar de lei de políticas públicas, onde o único crime é o de descumprimento de medida protetiva, a tipificação de tal conduta poderá inibir pessoas a cometerem esse ilícito.

7. RESPONSABILIDADE PENAL NOS CRIMES COM INTELIGÊNCIA ARTIFICIAL

Nesse capitulo será abordado sobre a responsabilidade penal nos crimes com Inteligência Artificial, levantando alguns pontos sobre a criação de novas leis para a tipificação dos delitos cometidos na internet, bem como qual procedimento utilizado na ação penal.

7.1. A necessidade de criação de normas penais para tipificar crimes na internet

Com relação a responsabilização do agente que utiliza Inteligência Artificial para cometer crimes na internet, ou também chamados de *cybercrimes*, se tem duas vertentes doutrinárias, uma que defende que esses crimes já estão tipificados no Código Penal Brasileiro, sendo a internet apenas um meio para a consumação dos delitos (Reis, 2021).

Quando o crime for cometido com o uso de Inteligência Artificial, essa seria apenas uma facilitadora para um crime que já está tipificado em nosso ordenamento jurídico, nas palavras de Patrícia Peck Pinheiro (2021, p.223):

> A maioria dos crimes cometidos na rede ocorre também no mundo real. A Internet surge apenas como um facilitador, principalmente pelo anonimato que proporciona. Portanto, as questões quanto ao conceito de crime, delito, ato e efeito são as mesmas, quer sejam aplicadas para o Direito Penal ou para o Direito Penal Digital.

Porém outra corrente doutrinária, entende que o fato de não se ter uma tipificação própria para crimes virtuais, se tem usado de analogia *in malam partem* para punir tais condutas. (Reis, 2021).

Os doutrinadores Damásio de Jesus e Jose Antônio Milagre abordam o princípio da legalidade quanto a questão da criação de normas para a regularização e responsabilidade nos crimes na internet.

> O Brasil adota o sistema da reserva legal. Não há crime, sem lei anterior que o defina. Especialmente quando tratamos de tecnologia da informação, a técnica para criar leis deve ser outra. Isto porque o legislador deve ter o cuidado para que não conceba uma ordenação jurídica natimorta, que ingressa no arcabouço legislativo de modo ultrapassado (Jesus; Milagre, 2016, p.12)

Dentre as classificações do crime, se tem quanto a forma de sua prática, onde os crimes cometidos com o uso de Inteligências Artificiais, pode-se dizer que se trata de crime de forma vinculada, pois a internet não é o meio para o cometimento do crime, e sim a forma em que ele pode ser praticado.

Segundo o pensamento de Tarcísio Teixeira (2022, p.184):

> Ora, se a inteligência artificial tem por objetivo, conforme previamente exposto, executar tarefas próprias da natureza humana, em determinado momento pode ocorrer uma situação em que as máquinas ajam de forma imprevisível – tal como ocorre com os seres humanos, que não raras vezes tomam decisões inesperadas e descumprem as normas éticas, sociais e jurídicas –, daí a necessidade de regulamentar o uso da inteligência artificial.

Os chamados crimes virtuais têm cada vez mais aumentado no Brasil, que vão desde invasão de dispositivos eletrônicos, a modificação de fotos e vídeos, com o objetivo de prejudicar outrem.

Nesse sentido, cabe lembrar da Teoria Tridimensional do Direito de Miguel Reale

> Onde quer que haja um fenômeno jurídico, há, sempre e necessariamente, um fato subjacente (fato econômico, geográfico, demográfico, de ordem técnica etc.); um valor, que confere determinada significação a esse fato, inclinando ou determinando a ação dos homens no sentido de atingir ou preservar certa finalidade ou objetivo; e, finalmente, uma regra ou norma, que representa a relação ou medida que integra um daqueles elementos ao outro, o fato ao valor (Reale, 2002, p. 59).

O aumento desses crimes destaca a extrema importância de uma legislação específica e totalmente voltada para esses tipos de delitos, que são cometidos diariamente na web. É essencial que essa norma, além de definir claramente os crimes, também forneça os instrumentos necessários para que o Executivo e o Judiciário possam efetivamente aplicá-la (Reis, 2021).

Os crimes na internet com o uso de Inteligências Artificiais, já se tem a valorização negativa por parte da sociedade. Portanto, seguindo esse caminho, o próximo passo seria a criação da norma que trate sobre a responsabilidade penal desses delitos.

7.2. Ação Penal nos crimes contra a honra cometidos com o uso de IA

Atualmente no direito penal brasileiro, os crimes contra a honra tipificados nos artigos 138, 139 e 140, ambos do Código Penal, porém, esse mesmo dispositivo no artigo 145 dispõe que esses crimes se procedem por queixa crime.

> Art. 145 - Nos crimes previstos neste Capítulo somente se procede mediante queixa, salvo quando, no caso do art. 140, § 2º, da violência resulta lesão corporal (Brasil, 1940).

Sendo necessário que a vítima forneça a qualificação do agente que comete tais crimes, ou mesmo, características e informações necessárias para que se possa identificá-lo, porém, muitas vezes criminosos usam de anonimato, ocultando o seu ID na internet.

Outra questão que se deve ser abordada é a competência para julgar os crimes cometidos na internet. Sendo necessário estabelecer onde se tem a consumação dos crimes cometidos contra a honra usando as Inteligências Artificiais.

O sistema penal brasileiro adota a teoria do resulto, sendo assim, a competência para julgar o delito seria o local onde ocorreu o delito, conforme o Código de Processo Penal, que

diz “Art. 70. A competência será, de regra, determinada pelo lugar em que se consumar a infração, ou, no caso de tentativa, pelo lugar em que for praticado o último ato de execução” (Brasil, 1941).

Ocorre que a internet não encontra fronteiras, onde o agente pode cometer crimes contra honra com as IAs, como exemplo as *deepfakes*, onde o agente pode ofender o bem jurídico de outrem em outro estado da União. O que se faz necessário abordar em legislação própria sobre o tema devido a complexibilidade do procedimento a ser aplicado.

No caso dos crimes contra a honra, que são considerados de natureza formal, apenas o último critério é aplicável. Porém, quando esses crimes acontecem na internet, identificar o local onde o crime foi consumado se torna mais difícil. Isso se deve ao fato de que o acesso à internet por meio de dispositivos móveis é muito fácil, o que facilita tanto a publicação das postagens quanto o acesso a elas, que é imediato e sem restrições (Rosa; Moser, 2022).

Conforme as palavras de Cattani, resume a problemática da regulamentação e a responsabilidade penal nos crimes cometidos com o uso de Inteligências Artificiais.

> A questão aqui não é se deve haver uma regulamentação, pois resta evidente sua necessidade. No entanto, não basta somente criminalizar ou proibir por texto de lei. É preciso que haja o engajamento dentro de um sistema legal e regulatório que seja efetivo, rápido, assegure a liberdade sem censura e, ao mesmo tempo, seja eficaz no monitoramento, avaliação, controle, remoção de conteúdo e punição dos infratores (Cattani, 2024).

Para concluir, foi demonstrado a importância da criação de novas normas, a fim de tipificar crimes cometidos com o uso de Inteligência Artificial, onde ao criar leis especificas, resolvendo possíveis conflitos de normas, onde de acordo com o princípio da especialidade, bem como, ao ter uma norma própria, é possível adequar a conduta ao tipo penal, garantindo assim, que o agente que comete delitos com Inteligência Artificial venha a ser responsabilizados.

CONCLUSÃO

Analisando as colocações, é possível concluir que antes da Lei dos Crimes Cibernéticos, não se tinha a tipificação especifica de delitos cometidos em ambiente virtual, sendo utilizado de analogia os delitos já descritos no Código Penal Brasileiro.

Entretanto, com o surgimento acelerado de novas tecnologias, as Inteligências Artificiais cada vez com capacidade de alterar fotos, vídeos e áudios, aliado ao fato de que uma

enorme parcela da população usa as redes sociais, as quais tem um grande potencial de propagação de conteúdo.

Cabe relembrar a Teoria Tridimensional de Miguel Reale, onde se tem o fato, posteriormente esse fato é valorado pela população, ou pelo judiciário, consequentemente se tem o surgimento da norma que regula, ou prevê punição para tal fato.

Os casos de crimes de informática, com o uso de IA tem se tornado cada vez mais comum, porém não se tem normas especificas que preveem a responsabilidade penal do agente que comete tal delito.

Em um panorama geral, o legislativo brasileiro tem apresentado projetos de lei, a fim de regulamentar o uso e desenvolvimento das Inteligências Artificiais no Brasil, a fim de buscar uma segurança jurídica, e a punibilidade dos ilícitos cometidos. Porém, por se tratar de um tema extremamente complexo, tem se buscado estudos, a fim de criar uma lei que não se torne obsoleta em pouco tempo.

As Inteligências Artificiais podem ser utilizadas para causar danos a diferentes bens jurídicos tutelados na Constituição Federal de 1988, e em leis infraconstitucionais. No entanto, porém se faz adequar o crime cometido com a internet, com alguma das condutas já tipificada no Código Penal.

Cabe destacar que o legislativo, a passos lentos busca uma regulamentação das Inteligências Artificiais no Brasil, com projetos de lei, que em seu texto prevê sansões penais em crimes cometidos com o uso dessa tecnologia.

Portanto, se faz necessário a implementação de normas especificas para a tipificação dos crimes cometidos na internet com o uso de Inteligências Artificiais, para que seja possível toda a persecução penal, dando ferramentas, para as partes e o magistrado poderem dar seguimento ao processo dentro da legalidade.

Por fim, este artigo discutiu a responsabilidade penal nos delitos cometidos com o uso de Inteligências Artificiais, para que se tenha uma segurança jurídica, bem como a aplicação da lei penal, buscando punir tais crimes e, por meio disso, acabar inibindo com que outras pessoas venham a praticar tais condutas, devido ao receio de uma condenação.

Este trabalho se propôs a levantar esses questionamentos e apresentar o tema, porém, sem esgotar a questão que vai ser decidida principalmente com a aprovação dos projetos de lei

que tipificam os crimes cometidos com Inteligências Artificiais. Assim, este trabalho se encerra, em grande medida, cumprindo seu papel.

REFERÊNCIAS

ANDRADE, Lisane. Quais são os 4 tipos de inteligência artificial? Conheça os detalhes e Aplicações Práticas, **Niara**, 29 de junho de 2024, Disponível em: https://niara.ai/blog/tipos-de-inteligencia-artificial/, Acesso em 19 out. 2024.

ARAS, Vladimir. A inteligência artificial e a potencialização das fraudes em geral. **Consultor Jurídico**, 27 de março de 2024. Disponível em: https://www.conjur.com.br/2024-mar-27/a-inteligencia-artificial-e-a-potencializacao-das-fraudes-em-geral/, Acesso em 17 nov.2024.

ARAÚJO, Janaína. Dez anos de vigência da Lei Carolina Dieckmann: a primeira a punir crimes cibernéticos. **Rádio Senado,** 2023. Disponível em: https://www12.senado.leg.br/radio/1/noticia/2023/03/29/dez-anos-de-vigencia-da-lei-carolina-dieckmann-a-primeira-a-punir-crimes-ciberneticos#:~:text=Dos%20seis%20meses%20a%20dois,Da%20R%C3%A1dio%20Senado%2C%20Jana%C3%ADna%20Ara%C3%BAjo, Acesso em: 15 out. 2024.

ARRUDA, Felipe. 20 anos de internet no Brasil: aonde chegamos? **Tecmundo**, 2011. Disponível em: https://www.tecmundo.com.br/internet/8949-20-anos-de-internet-no-brasil-aonde-chegamos-.htm. Acesso em: 11 set. 2024.

BRASIL. Lei 12.965, de 23 de abril de 2014, Marco Civil da Internet, Brasília, DF: **Diário Oficial da União,** 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 21 set. 2024.

BRASIL. Lei 12.737, de 30 de novembro de 2012. Lei dos crimes cibernéticos, Brasília, DF: **Diário Oficial da União**, 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em:21 set. 2024.

BRASIL. Decreto-lei 2.848, de 7 de dezembro de 1940. Código Penal, Brasília, DF: **Diário Oficial da União**, 1940. Disponível em:https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm, acesso em:15 set 2024.

BRASIL. Decreto-lei 3.689, de 03 de outubro de 1941. Código de Processo Penal, Brasília, DF: **Diário Oficial da União**, 1941. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em: 15 set. 2024.

BRASIL, Senado Federal. **Projeto de Lei 2.338/2023.** Dispõe sobre o uso da Inteligência Artificial. 2023, Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/157233. Acesso em:11 out. 2024.

CÂMARA DOS DEPUTADOS. **Projeto de lei 5.695 de 2023**, disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2406516#:~:text=PL%205695%2F2023%20Inteiro%20teor,Projeto%20de%20Lei&text=Tipifica%20penalmente%20a%20altera%C3%A7%C3%A3o%20de,praticar%20viol%C3%AAncia%20contra%20a%20mulher, Acesso em: 20 set. 2024.

CÂMARA DOS DEPUTADOS, **Projeto de Lei 21 de 2020**, disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2236340. Acesso em: 20 set. 2024.

CASTRO, André Zanatta Fernandes; MARQUES, Fernanda Mascarenhas; KAUFFMAN, Bernardo Fernandes. A regulamentação da IA nos EUA e no Reino Unido, **Jota**- 2024, Disponível em: https://www.jota.info/artigos/a-regulamentacao-da-ia-nos-eua-e-no-reino-unido. Acesso em 28 nov. 2024.

CATTANI, Federico. Uso da inteligência artificial como ferramenta para criminalidade. **Consultório Jurídico**, 11 de fev. de 2024. Disponível em: https://www.conjur.com.br/2024-fev-11/uso-da-inteligencia-artificial-como-ferramenta-para-criminalidade/. Acesso em: 28 set. 2024.

COMISSÃO EUROPEIA. Proposta de Regulamento do Parlamento Europeu e do Conselho que estabelece Regras Harmonizadas em Matéria de Inteligência Artificial (Regulamento Inteligência Artificial) e Altera determinados Atos Legislativos da União. COM/2021/206 final. Publicado em 21 de abril de 2021. **EUR-Lex**. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52021PC0206. Acesso em 10 out. 2024.

HOMEWORK. Como a IA está sendo usada como ferramenta do cibercrime. **Terra**, Disponível em: https://www.terra.com.br/byte/seguranca-digital/como-a-ia-esta-sendo-usada-como-ferramenta-do-cibercrime,37f557299f82b0285824409cf6469589j1is5wj9.html. Acesso em 03 nov. 2024.

JESUS, Damásio de; MILAGRE, Jose Antônio. **Manual de crimes informáticos**. São Paulo – Saraiva, 2026.

MIYASHIRO, Kelly. De Bonner a Pedro Bial: os famosos que viraram vítimas da nova deep fake. **Veja**, 18 de jan. de 2024. Disponível em: https://veja.abril.com.br/coluna/tela-plana/de-bonner-a-pedro-bial-os-famosos-que-viraram-vitimas-de-nova-deep-fake. Acesso em 20 nov. 2024.

PINHEIRO, Patrícia Peck. **Direito digital**. 7. ed. São Paulo: Saraiva Educação, 2021. e-book.

QUEIROZ, João Quinelato de. **A responsabilidade civil dos provedores de aplicações de internet por danos decorrentes de conteúdo gerado por terceiros: análise na perspectiva civil- constitucional**. Universidade Estadual do Rio de Janeiro. Dissertação de Mestrado. 2018. Disponível em: http://www.bdtd.uerj.br/handle/1/9862. Acesso em: 21 out. 2024.

REALE, Miguel. **Lições preliminares de direito**. 27. ed. São Paulo: Saraiva, 2002.

REIS, Caio Gonçalves. Crimes virtuais: Uma análise acerca da (in) eficácia da legislação e os desafios de sua persecução penal. **Jus Brasil**, 2021. Disponível em: https://www.jusbrasil.com.br/artigos/crimes-virtuais-uma-analise-acerca-da-in-eficacia-da-legislacao-e-os-desafios-de-sua-persecucao-penal/1220973039#:~:text=Nesses%20casos%2C%20a%20picha%C3%A7%C3%A3o%20pressup%C3%B5e,simetria%2C%20a%20condutas%20inform%C3%A1ticas%20criminosas. Acesso em: 13 out. 2024.

RIVELLI, Fabio; SILVEIRA, Ricardo Freitas, Regulação chinesa para sistemas generativos de IA pode influenciar o ocidente? **Migalhas**, 2023. Disponível em: https://www.migalhas.com.br/coluna/ia-em-movimento/390836/regulacao-chinesa-para-sistemas-de-ia-pode-influenciar-o-ocidente. Acesso em: 10 out. 2024.

ROSA, Fabrízio. **Crimes de Informática**. 2ª. ed. Campinas: Bookseller, 2005.

ROSA, Luísa Walter da; MOSER, Manuela. Competência para julgamento de crimes contra a honra praticados pela internet: necessidade de revisão da jurisprudência. **Migalhas**, 2023. Disponível em: https://www.migalhas.com.br/depeso/372837/competencia-para-julgamento-de-crimes-contra-a-honra-na-internet. Acesso em: 15 nov.2024.

SALESFORCE BRASIL. **Deep e Machine Learning: qual a diferença?** - 2024, Disponível em: https://www.salesforce.com/br/blog/machine-learning-vs-deep-learning/. Acesso em: 25 out. 2024.

TAYLOR SWIFT e eleições: Entenda como a IA se tornou ameaça eleitoral, **Migalhas**, 06 de fev. de 2024. Disponível em: https://www.migalhas.com.br/quentes/401301/taylor-swift-e-eleicoes-entenda-como-a-ia-se-tornou-ameaca-eleitoral. Acesso em 15 nov.2024.

TEFFÉ, Chiara Antonia Spadaccini. A responsabilidade civil do provedor de aplicações de internet pelos danos decorrentes do conteúdo gerado por terceiros, de acordo com o Marco Civil da Internet. **Revista Fórum de Direito Civil,** v. 4, n. 10, 2015. Disponível em: https://editoraforum.com.br/wp-content/uploads/2015/12/A-responsabilidade-civil-do-provedor-de-aplicacoes-de-internet.pdf. Acesso em: 13 out. 2024.

TEIXEIRA, Tarcísio. **Direito Digital e Processo Eletrônico.** 6a. ed. São Paulo: SaraivaJur, 2022.