CASO TABATA AMARAL: O USO DA INTELIGÊNCIA ARTIFICIAL E SUA REPERCUSSÃO PENAL

Ana Clara da Cruz Araújo de Souza[1]
João Batista Machado Barbosa[2]

RESUMO

O objetivo do presente artigo é o estudo do caso concreto envolvendo a Deputada Federal Tabata Amaral, na qual foi vítima de um delito envolvendo as ferramentas de inteligência artificial, de maneira mais precisa, o "Deepfake". Trazendo uma importante discussão acerca do direito de imagem na atualidade e, de forma subsidiária, a repercussão penal e suas consequências em relação aos indivíduos que usam essas ferramentas tecnológicas para cometer crimes, com enfoque na ineficácia das leis atuais a fim de haver uma punição proporcional aos prejuízos causados. Ademais, busca-se refletir sobre a rápida evolução desses mecanismos e as consequências de seu uso indevido na sociedade moderna.

Palavras-chave: Tabata Amaral. Deepfake. Inteligência Artificial. Ineficácia.

TABATA AMARAL CASE: THE USE OF ARTIFICIAL INTELLIGENCE AND ITS CRIMINAL REPERCUSSION

ABSTRACT

The objective of this article is to study the specific case involving Federal Deputy Tabata Amaral, in which she was the victim of a crime involving artificial intelligence tools, more precisely, "Deepfake". Bringing an important discussion about image rights today and, in a subsidiary way, the criminal repercussions and their consequences in relation to individuals who use these technological tools to commit

[1] Acadêmica do curso de Direito do Centro Universitário do Rio Grande do Norte - UNI/RN. Email: 2021A037011@a.unirn.edu.br
[2] Professor Orientador do curso de Direito do Centro Universitário do Rio Grande do Norte - UNI/RN. Email: jbmb@unirn.edu.br

crimes, focusing on the ineffectiveness of current laws in order to have a proportional punishment to the damage caused. Furthermore, we seek to reflect on the rapid evolution of these mechanisms and the consequences of their misuse in modern society.

Keywords: Tabata Amaral. Deepfake. Artificial Intelligence. Ineffectiveness.

1. INTRODUÇÃO

O progresso da inteligência artificial e a rápida evolução de novas técnicas como o “deepfakes” permitem a manipulação, produção de conteúdos falsos de vídeos, áudios e imagens que são muito parecidos com o conteúdo original e, com a rapidez dos avanços tecnológicos, torna-se quase imperceptível as falhas das ferramentas de inteligência artificial, levantando o questionamento do que realmente é real e o que é manipulado digitalmente. Embora tenha várias vantagens, seu uso impróprio é alarmante. As deepfakes se transformaram numa ferramenta eficaz para influenciar ou manipular. Tornando-se uma importante ferramenta para a distorção da verdade, seja no contexto político ou social, fazendo com que a tecnologia se torne uma extensão das notícias falsas ou “artilharia” para a propagação de uma variação de crimes.

Persuadir indivíduos, distorcer opiniões, prejudicar a reputação de indivíduos e entidades, influenciar e obter influência. O uso desses mecanismos de inteligência artificial provocaram uma autêntica transformação tecnológica nos conteúdos de notícias falsas. “A disseminação acelerada de conteúdos alterados e de alta qualidade torna mais difícil detectar fraudes e adulterações”. (Korshunov & Marcel, 2019). Ao longo dos anos, esses conteúdos se tornarão tão exatos que ficou complicado determinar se são autênticos, a perfeição dos detalhes tornou-se uma grande incógnita para os peritos desvendarem, trazendo a reflexão do que realmente é real nas redes sociais, tendo em vista os altos padrões da sociedade em busca da perfeição idealizada.

Em pesquisa realizada pela Kaspersky, em parceria com a empresa de pesquisa CORPA, 66% dos brasileiros têm total desconhecimento sobre a técnica de deepfake e 71% não reconhece quando um vídeo foi editado a partir de tal mecanismo, tal resultado pode colaborar no sucesso de fraudes. Segundo Dmitry Bestuzhev, diretor da

equipe global de pesquisa e análise da Kaspersky na América Latina, em depoimento para a pesquisa, “À medida que a tecnologia se torna menos cara, podemos esperar o surgimento de seu uso ilícito”.

Ou seja, a partir do momento em que a tecnologia e suas inovações tornam-se acessíveis a todos, fica suscetível o seu uso indevido por uma parte da camada da sociedade, a falta da regulação dessas ferramentas torna sua utilização uma “terra sem lei”, onde a criatividade é ilimitada. O leque de possibilidades para cometer delitos usando de tal mecanismo é imenso e, diante disso, no Brasil a punição não é proporcional ao prejuízo causado em muitos casos concretos, principalmente se levar em conta a qualidade de tais ferramentas, onde as mesmas buscam beirar as perfeições de detalhes, sendo um árduo trabalho detectar as mínimas falhas e, quando tal comprovação é feita, geralmente o caos já foi propagado, tendo em vista a velocidade do acesso à informação atualmente. Diversos direitos podem ser violados a partir de uma simples montagem, mas a legislação brasileira ainda não está preparada para aplicar o princípio da proporcionalidade na hora de punir os criminosos responsáveis pelos atos.

De maneira geral, neste artigo, o foco será no caso concreto escolhido e as consequências geradas em decorrência do uso inapropriado da inteligência artificial, evidenciando a utilização para disseminar informações falsas a fim de desestabilizar a vítima. Ademais, serão analisadas as consequências de sua aplicação indiscriminada e/ou sem algum tipo de caracterização explícita e/ou controle, e não a partir de seu desenvolvimento técnico ou seus propósitos científicos. O objetivo do presente artigo é contextualizar as deepfakes no âmbito do problema da realidade sintetizada/simulada (a manipulação digital de fato) e relacioná-lo com o problema da verdade. Assim como, objetivando o aprofundamento dos estudos sobre a técnica deepfake discutindo o uso indevido de tal tecnologia e quais são as soluções existentes para combatê-la, a partir da regulação do uso, tal como, a evolução e andamento das atuais medidas de combate/punição para os atos praticados, com foco na repercussão penal e a violação de direitos fundamentais garantidos pela Constituição Federal como, por exemplo, o uso indevido da imagem. Tendo como base as pesquisas acadêmicas, decisões de tribunais e jurisprudências pacificadas.

2. CONCEITO E EVOLUÇÃO HISTÓRICA DO DEEPFAKE

O termo “deepfake” surgiu em 2017 quando um usuário do Reddit usou o apelido “deepfakes” para postar vídeos pornográficos alterados digitalmente - mediante as ferramentas “primatas” da I.A da época -, com imagens de celebridades (algo se tornou extremamente comum na atualidade). “A tecnologia foi aplicada usando como base inúmeras imagens e vídeos de celebridades para aprender a imitar as expressões faciais e sobrepor em um vídeo o rosto de uma celebridade no rosto de atrizes de filmes pornô” (Hall, 2018).

A descrição para definir o deepfake seria a manipulação digital de som, imagens ou vídeo para imitar alguém ou fazer parecer que a pessoa fez alguma coisa e, objetivando no futuro fazer isso de uma maneira que seja cada vez mais realística, a ponto de um observador desavisado não conseguir detectar a falsificação, assim como o grau tão elevado de realidade que faz com que seja quase impossível se detectar a fraude, o que é especialmente perigoso nos tempos atuais, marcado pela “economia da atenção”, onde atividades cognitivas que exija muita atenção aos detalhes (como é o caso da detecção de imagens falsas), tornaram-se um empecilho na vida da população mais jovem. Onde o “imediatismo” é soberano a qualquer outro aspecto da vida, ou seja, é mais cômodo acreditar imediatamente naquilo que visualizou inicialmente do que buscar a veracidade dos fatos ou questionar a realidade.

O aperfeiçoamento, desenvolvimento acelerado e aplicações de novas tecnologias sempre supera o que era imaginado a princípio, e hoje as tecnologias deepfake, que estão baseadas em deep learning (um ramo da aprendizagem de máquina) e que aplicam simulações de redes neurais a conjuntos massivos de dados (big data) são capazes de criar, por exemplo, pessoas que nunca existiram no “mundo real”, praticando atividades com extrema perfeição, obrigando os indivíduos a questionar se aquilo é realmente falso, afastando a hipótese do vale da estranheza que, “é um conceito que descreve a aversão que as pessoas sentem quando objetos artificiais se tornam muito parecidos com humanos, mas não idênticos” (Masahiro Mori, 1970).

Ademais, no Brasil o termo se popularizou em 2018, devido ao cenário político polarizado, podendo ser considerado como o “berço” da fake news no país e, consequentemente, do deepfake. Onde as ferramentas eram usadas para propagar notícias falsas em relação aos candidatos a representação do povo, gerando uma rede

de desinformação sem precedentes, gerando diversos prejuízos em relação a confiabilidade de qualquer notícia gerada na época, seja verdadeira ou falsa.

Ainda, de acordo com relatório da empresa Sensity (2019), 96% dos vídeos deepfake disponíveis na internet são de conteúdo pornográfico não consensual, e têm como alvo as mulheres, na maioria celebridades, assim como pessoas comuns. Outra grande problematização é o uso para construção de pornografia não consensual, ou como forma de vingança de ex-companheiros, ou como extorsão, chantagem, estelionato, dentre outros crimes. Já que grande parte dos conteúdos falsos encontrados na internet são de cunho pornográfico. Além do leque de possibilidade dos crimes acima citados, a nova "tendência" é gerar vídeos e fotos com conotação sexual de pessoas comuns, através de material colhido mediante as redes sociais, e chantagear as pessoas. Além de vídeos de falsos sequestros, também com material colhido das redes sociais, e extorquir terceiros em troca de suposto resgate.

Diante do exposto, fica evidente a "arma" de alta periculosidade que está disponível na internet, para que qualquer pessoa mal intencionada acesse, sendo a criatividade o limite do que podem fazer. Dessa forma, faz-se necessário a regulação do uso, além de novas políticas de proteção de dados pessoais e a devida responsabilização das empresas responsáveis pela criação e liberação livre, sem o devido cuidados com as consequências geradas a partir do uso desmedido e indevido.

3. CASO TABATA AMARAL

O caso escolhido para dissecar no presente artigo foi o da Deputada Federal, Tabata Amaral - atualmente, candidata a prefeita pela cidade de São Paulo, pelo partido PSB -, que foi uma infeliz vítima de crimes envolvendo a inteligência artificial, mais especificamente, o deepfake.

Ocorre que, entre os meses de agosto e setembro de 2024, foram vazadas supostas fotos sensuais da Deputada Federal, claramente com uma conotação sexual, gerando uma imensa repercussão nas redes sociais, tendo em vista a reputação séria da Parlamentar e, como já citado neste artigo, há maiorias dos brasileiros não conseguem diferenciar as fotos geradas por inteligência artificial e a realidade, causando uma comoção em massa diante de tal suposto vazamento de fotos. Diante dos acontecimentos, a reputação da Deputada foi afetada, sua honra manchada, trazendo

severas consequências a sua campanha política.

O ato foi praticado com a clara intenção de prejudicar sua campanha política, já que, segundo o portal G1, as fotos foram publicadas com a seguinte legenda: "Tabata Cláudia Amaral de Pontes é uma politóloga, ativista pela educação e política brasileira filiada ao Partido Socialista Brasileiro (PSB). Atualmente exerce o mandato de deputada federal pelo estado de São Paulo". Uma clara satirização em relação a Deputada, a fim de a desmerecer e desestabilizar sua “corrida” eleitoral pela prefeitura de São Paulo, diminuindo seu papel como representante do povo e, sobretudo, uma mulher que trilhou um árduo caminho para se sobressair no cenário político brasileiro.

No entanto, ainda segundo o portal G1, apesar da assustadora semelhança com a realidade, alguns peritos conseguiram encontrar alguns mínimos detalhes falhos, como, por exemplo, em uma das fotos (mais especificamente a de maiô), por exemplo, a ferramenta de detecção de I.A. analisou que o comprimento e as proporções das pernas parecem exageradas em comparação à anatomia humana comum.

Ainda, foi destacado por alguns peritos que a I.A. tem dificuldades em acabamentos, como, por exemplo, como mãos, cabelos, dedos e bordas. No entanto, é importante ressaltar que com os diversos aprimoramentos de tais ferramentas digitais, fica a assustadora reflexão sobre até quando ainda existirão esses mínimos erros e, a partir disso, passam a serem elaboradas com perfeição. O que parece uma realidade distópica, pode está se tornando real. Restando somente o sentimento de insegurança, perante a fragilidade dos dados pessoais dos indivíduos, tendo em vista que somente uma foto é necessária para gerar danos inimagináveis na vida de uma pessoa inocente, trazendo severas consequências.

Diante dos recorrentes casos de manipulação digital, a jurisprudência pacificou-se em relação a proibição do uso dessas ferramentas no período eleitoral, como fica demonstrado na seguinte decisão:

> Ementa: MANDADO DE SEGURANÇA. DECISÃO PROFERIDA PELO JUÍZO ELEITORAL. INDEFERIMENTO DE PEDIDO LIMINAR EM REPRESENTAÇÃO ELEITORAL. PRELIMINAR DE INÉPCIA DA PETIÇÃO INICIAL. AUSÊNCIA DE DEGRAVAÇÃO E ÍNTEGRA DE VÍDEO. REJEIÇÃO. MÉRITO. UTILIZAÇÃO DE INTELIGÊNCIA ARTIFICIAL (IA). DEEP FAKE EM PERÍODO PRÉ-ELEITORAL. IMPOSSIBILIDADE. VEDAÇÃO TOTAL, INDEPENDENTEMENTE DE INDUZIR O ELEITORADO A ERRO. CONCESSÃO DA SEGURANÇA. I. CASO EM EXAME Coligação partidária impetrou mandado de segurança contra decisão do Juízo Eleitoral que indeferiu pedido liminar em representação eleitoral. A decisão contestada rejeitou o pedido liminar da coligação, que apontava prática de

> deep fake em vídeo publicado pelos candidatos a prefeito e vice-prefeito. No vídeo, foi utilizada a imagem manipulada digitalmente do avô falecido de um dos candidatos, o que foi alegado como violação das normas eleitorais. A petição inicial da coligação impetrante foi alvo de preliminar de inépcia pela parte adversa, sob o argumento de ausência de degravação e integra do vídeo impugnado. II. QUESTÕES EM DISCUSSÃO A principal questão discutida refere-se à admissibilidade e validade da petição inicial, em função da alegada inépcia por falta de documentos essenciais, e à possibilidade de utilização de conteúdos produzidos por inteligência artificial, como deep fakes, em período pré eleitoral, mesmo com aviso sobre o uso de IA. III. RAZÕES DE DECIDIR 1. Preliminarmente, rejeitou-se a alegação de inépcia da petição inicial, uma vez que o vídeo impugnado foi disponibilizado via link na petição inicial e estava devidamente acessível, não sendo imprescindível a degravação ou juntada da íntegra do vídeo. **2. No mérito, a utilização de deep fakes em período pré-eleitoral foi considerada vedada, independentemente de o conteúdo ser claramente identificado como manipulado por inteligência artificial. A Resolução TSE n° 23.610/2019, com as modificações introduzidas pela Resolução n° 23.732/2024, impõe a proibição total do uso de deep fakes, tanto para prejudicar quanto para favorecer candidaturas, em razão do potencial de tais práticas para desequilibrar o pleito ou comprometer a integridade do processo eleitoral.** IV. DISPOSITIVO E TESE Diante do exposto, concede-se a segurança, anulando-se a decisão que indeferiu a liminar nos autos da Representação, **mantendo-se a vedação ao uso de deep fakes em conteúdos eleitorais, mesmo no período pré-eleitoral, conforme as normas eleitorais vigentes.** (TRE-MG - MANDADO DE SEGURANÇA CÍVEL: MSCiv XXXXX-47.2024.6.13.0000 UBERLÂNDIA - MG XXXXX - 22/08/2024).

No entanto, mesmo com decisões que garantem a vedação desses mecanismos de manipulação, não há de fato um controle ou um sistema próprio para apurar os casos, tornando-se ineficaz na punição efetiva para os responsáveis.

Ou seja, uma simples imagem publicada nas redes sociais pode gerar uma repercussão gigante, como o caso da Deputada Federal, onde seu direito à imagem foi violado e denegrido perante a população brasileira, a fim de degradar sua história política e desmoralizar sua honra perante a sociedade que, até o presente momento, ainda encontra-se sem resolução, pois os responsáveis não foram identificados.

São casos semelhantes ao em tela que incentivam a criação do presente artigo, onde o objetivo é buscar trazer uma reflexão sobre a insegurança dos dados pessoais, do direito à privacidade e à imagem. Questionar como um ato danoso como esse, sofre uma punibilidade tão desproporcional aos prejuízos causados, além de discorrer sobre a liberdade ao acesso de dados pessoais, sendo a criatividade o limite para fazer uso de tal material como bem entender. De acordo com Scott, Daniella (2020):

> "A humilhação pública decorrente do uso de deep fakes pode ser devastadora, especialmente para as mulheres, que muitas vezes enfrentam uma dupla penalização: a exposição de sua imagem e a desconfiança social sobre sua veracidade. Esses crimes ultrapassam o âmbito digital, gerando consequências

psicológicas e profissionais irreparáveis."

De maneira geral, será através desse caso concreto supracitado, que tal artigo irá dissecar, através de estudos e pesquisas, sobre o que é realidade sintetizada/simulada e o que real e, como isso pode afetar a vida do homem médio. Além de buscar saídas punitivas para a "terra sem lei" que se tornou essas ferramentas artificiais, tal como, discutir sobre as medidas que já existem contra tais atos praticados a partir da manipulação digital.

Por fim, é necessário uma conscientização do tema frente à sociedade brasileira, tendo em vista como apontado nas pesquisas citadas, o alarmante número de pessoas que repassam fake news sem ao menos verificar a veracidade da fonte ou tal informação, esquecendo ou apenas ignorando que deve existir uma responsabilidade na hora de disseminar informações. Não podendo se esconder "atrás" da liberdade de expressão, principalmente quando há a violação da honra de outrem e, sobretudo, quando há interesse público legítimo. Com a ampla disseminação de "fake news", a liberdade de expressão para poder ser permitida deve guardar pertinência com a realidade, evitando-se gerar um desfavor contra a sociedade e a propagação de ideias falsas gerando uma rede de desinformação.

4 A LEGISLAÇÃO INAPTA E A INEFICIÊNCIA NO CONTROLE DA I.A.

3.1 LEGISLAÇÃO

A Legislação Brasileira não criminaliza especificamente o "DeepFake'. Mas os intérpretes do direito tem buscado amparo em tipos penais descritos na Lei Federal n.º 12.735/2012 (Lei Azeredo); Lei Federal n.º 12.737/2012 popularmente conhecida como Lei Carolina Dickmann; Lei Federal n.º 12.965/2014 (Marco Civil da Internet); Lei Federal n.º 13.718/2018 oriunda do Projeto de Lei n.º 5.555/2013; Lei Federal n.º 13.709/2018 - Lei Geral de Proteção de Dados Pessoais; Lei Federal n.º 13.853/2019. Além dos tipos penais descritos na Lei de Crimes Financeiro (Lei Federal n.º 7.492/86); Lei de Falências (Lei Federal n.º 11.101/2005); Código Eleitoral (Lei Federal n.º 4737/65) e principalmente nos crimes contra a honra (artigos 138/145 do Código Penal) e dignidade sexual (artigos 213/235 'c' do Código Penal).

Diante da falta de uma norma específica, o Ministro do Superior Tribunal de

Justiça (STJ), Ricardo Villas Bôas Cueva pontuou que o Marco Civil está atrasado no que toca ao combate à desinformação e que uma das possivéis alternativas para o combate de (Deep) fake news seria:

> "A criação de um algoritmo capaz de detectar o que é ou não fakenews, mas obviamente isso geraria ainda mais críticas. Quem controla a caixa-preta do algoritmo e determina os parâmetros do que é falso ou verdadeiro?"

Além disso, no âmbito criminal, recentemente, o Código Penal foi reformado para abarcar também a criminalização das montagens de deep fakes que incluam a pessoa em cena de nudez ou de ato sexual ou libidinoso de caráter íntimo, conforme a dicção expressa do parágrafo único do art. 216-B:

> Art. 216-B. Produzir, fotografar, filmar ou registrar, por qualquer meio, conteúdo com cena de nudez ou ato sexual ou libidinoso de caráter íntimo e privado sem autorização dos participantes: (Incluído pela Lei nº 13.772, de 2018) Pena - detenção, de 6 (seis) meses a 1 (um) ano, e multa. Parágrafo único. Na mesma pena incorre quem realiza montagem em fotografia, vídeo, áudio ou qualquer outro registro com o fim de incluir pessoa em cena de nudez ou ato sexual ou libidinoso de caráter ínti- mo. (Incluído pela Lei nº 13.772, de 2018)

Todos os artigos e leis supracitados tentam chegar a uma responsabilização (penal e cível) efetiva, próximo ao proporcional do dano causado pelo delito. No entanto, diante das "atualizações" constantes dos meios para os crimes digitais, se faz necessário um norma específica a fim de regular o uso e punir de forma proporcional a conduta danosa, somente de 06 meses a 1 ano de pena não é justo em comparação ao dano causado. Tal como, discutir a possibilidade da responsabilidade civil objetiva ou subjetiva, por parte das empresas criadoras das ferramentas, que permitem o acesso desordenado por qualquer cidadão comum, sem qualquer responsabilização pelo vazamento e uso indisciplinado dos dados pessoais (sem o consentimento) de terceiros.

Em meados de 2023, houve a proposta do projeto de lei n° 1272, com o intuito de tipificar adulteração maliciosa de vídeos ou áudios, onde, "Adulterar arquivos de vídeo ou de áudio, mediante clonagem da voz, substituição de rosto, sincronização labial ou outra ferramenta de inteligência artificial, com a intenção de divulgar notícias falsas ou prejudicar pessoa física ou jurídica", segundo o próprio texto do projeto de lei.

Ainda, segundo o advogado José Estevam Macedo Lima, especialista em crimes virtuais, esclarece: “Essa tecnologia não só é uma ameaça gravíssima ao mundo em geral, como pode mudar o destino e curso da vida de uma pessoa em âmbito pessoal e corporativo, assim como o destino e curso de toda uma empresa. Importante destacar que, por se tratar de uma tecnologia que distorce a realidade, através de Inteligência Artificial (IA), com objetivo de reproduzir fatos que jamais ocorreram e de atingir uma ou mais pessoas, não há, por enquanto, legislação específica que regulamente o tema no País”.

No entanto, apesar de ser um considerável avanço para a legislação brasileira, o projeto ainda não foi aprovado. Cabendo aos aplicadores do direito tentar buscar maneiras de punir e haver a reparação adequada para o delito cometido. Gerando a sensação de impunidade, por parte das vítimas, tendo em vista que diversos prejuízos sem precedentes foram causados, a imagem foi manchada, e seus direitos violados. Sendo injusto que usem e abusem da imagem alheia, sem o devido consentimento, e saiam impunes ou tenham uma punição desproporcional ao dano causado.

Como um caso que ocorreu com uma estudante da Austrália, em um dia comum, por curiosidade, decidiu procurar fotos suas na internet, para buscar menções ou postagens em sua referência nas redes sociais de amigos. O que lhe apareceu, contudo, foram centenas de imagens explícitas em que estava nua ou performando atos sexuais gráficos. Isso a deixou completamente desnorteada, já que nunca tinha tido sequer um namorado ou tirado aquelas fotos. Desesperada e constrangida com a exposição, buscou medidas para solucionar aquela situação, no entanto, foram medidas infundadas, tendo em vista que, na época, pouco se falava sobre o assunto, eram os primórdios da tais ferramentas de inteligência artificial, logo, não havia qualquer regulamentação ou tipificação para aquele ato.

Ocorre que, seis anos depois, o pesadelo se tornou maior, Noelle Martin descobriu então que havia feito uma deepfake com suas fotos, compartilhando mais de um vídeo em que aparece em cenas de sexo explícito, com legendas descritivas sobre o ato presente no vídeo, descrevendo com sexo real. Diante disso, a mesma chegou a afirmar que “Eu assisti enquanto meus olhos encaravam a câmera, enquanto minha própria boca se mexia. Era convincente, até para mim”, disse ela em entrevista.

Diante do exposto, ao considerar o caso concreto da jovem estudante australiana e o caso escolhido para estudo do presente artigo, da Deputada Federal

Tabata Amaral, torna-se evidente os prejuízos causados pelas práticas de crimes feitos a partir da utilização das ferramentas de inteligência artificial, os danos causados a essas mulheres, assim como muitas outras vítimas, é irreparável, tendo em vista que afeta sua dignidade, seu estado psicológico, viola seu direito à imagem, privacidade e, acima de tudo, as viola. Tal ato é humilhante, tendo em vista que esses vídeos e fotos com conotação sexual são usados para desqualificar essas mulheres, às resumindo ao papel de objeto sexual.

Esta problemática é relevante para discussão, especialmente se observado o contexto de anomia que impera na grande parte dos sistemas de justiça penal, cuja desproteção específica acaba por inspirar insegurança às vítimas e revitimização por carência de proteção estatal adequada, tendo em vista que, não bastasse sofrer por tal ato, ainda, devido ao processo legal, são obrigadas a reviverem várias vezes o mesmo momento, trazendo um dano psicológico evidente**,** sendo a humilhação o sentimento soberano, diante de tal situação.

Logo, diante dos fatos expostos, fica evidenciado a falha na legislação brasileira (ou até mesmo em outros países), diante da acelerada evolução das ferramentas de inteligência artificial, fica demonstrando a falta de eficácia no controle de disponibilidade e acesso desses mecanismos, faltando a tipificação penal proporcional ao ato danoso feito.

3.2 VIOLAÇÃO DO DIREITO À IMAGEM

Como já evidenciado, o uso desordenado dessas ferramentas geram consequências devastadoras para as vítimas e, com a vastidão que é a internet, muitas vezes é impossível identificar os responsáveis pela criação desses conteúdos. Inclusive, conteúdos esses que são elaborados a partir do uso não consentido da imagem de outrem.

A Constituição Federal do Brasil assegura o direito à imagem como um direito fundamental em seu artigo 5º, inciso X, que declara a inviolabilidade da honra e da imagem dos indivíduos. Este direito salvaguarda o indivíduo contra o uso indevido de sua imagem em qualquer meio de comunicação, sendo este comportamento visto como uma infração à sua privacidade e dignidade.

No ordenamento brasileiro, o direito à imagem é considerado um direito

personalíssimo, isto é, é um direito exclusivo do indivíduo, e sua violação pode acontecer de várias maneiras. Usar indevidamente a imagem de alguém, especialmente em ambientes digitais, onde a distorção da realidade pode ser realizada com extrema facilidade, é uma das formas mais graves de violação desse direito. Em situações de deep fake, o conteúdo manipulado, mesmo que baseado em imagens autênticas, é modificado para propósitos que o indivíduo retratado nunca deu seu consentimento. Portanto, a infração não é somente de natureza visual, mas também moral, pois impacta a reputação, a honra e a privacidade do indivíduo. Ainda, de acordo com Chesney, R., & Citron, D. K. (2019):

> "As deep fakes não são apenas uma ameaça tecnológica; elas são uma ameaça direta ao direito de uma pessoa à privacidade e à imagem, manipulando representações faciais e vocais para criar conteúdos que podem prejudicar a honra e a reputação, causando danos irreparáveis."

Como foi o caso da Deputada Federal, Tabata Amaral, sem o consentimento dela, pegaram algumas imagens de seu perfil público nas redes sociais e, a partir das ferramentas de I.A., criaram as imagens de cunho sexual para manchar sua honra e prejudicar sua candidatura política, aos olhos da sociedade e de seus eleitores, violando seu direito fundamental à imagem, garantido pela Constituição Federal.

O art. 20 do Código Civil traz a autorização/consentimento, como condição para a utilização da imagem de uma pessoa, ressalvadas as exceções trazidas pela própria lei. Menezes Cordeiro aponta semelhante solução no direito português, ao afirmar que "[o] artigo 79.º/1 consagra a regra básica: o retrato de uma pessoa não pode ser exposto, reproduzido ou lançado no comércio sem o consentimento dela". Ignorar esse direito viola diretamente a Constituição Federal.

A tecnologia de deep fake, apesar de sua força, representa um perigo considerável para a privacidade e a integridade dos indivíduos, especialmente quando empregada na manipulação de imagens e calúnias. A infração do direito à imagem por deep fakes é uma questão em ascensão que requer uma resposta mais efetiva da lei, das plataformas digitais e da sociedade como um todo.

É crucial a criação de políticas públicas e normas mais eficientes para combater os crimes digitais, assegurando que as vítimas estejam salvaguardadas e que os infratores sejam devidamente penalizados. Simultaneamente, é crucial fomentar a sensibilização acerca dos perigos da manipulação digital e instruir a população sobre

os riscos de consumir e compartilhar conteúdo sem conferir sua autenticidade, com o objetivo de salvaguardar os direitos básicos de todos na era digital.

3.3 CONVENÇÃO DE BUDAPESTE

Em meados do ano de 2001, alguns países europeus se juntaram para discutir a repercussão e os prejuízos causados pelos crimes cibernéticos, diante do constante crescimento de tais ações, tornou-se crucial dar acesso a essa discussão para outros países, a fim de buscar medidas efetivas para que haja uma punição adequada. Assim, surgiu a Convenção de Budapeste, como é conhecida até hoje.

Embora o período de assinaturas tenha sido aberto no final de 2001, há mais de 20 anos, a Convenção ainda é um dos assuntos mais relevantes. Buscando a discussão sobre uma agenda comum para cooperação Internacional em prol da luta contra delitos praticados no meio digital exercido influência em leis globais.

A Convenção sobre o Cibercrime aborda temas como (i) criminalização dessas ações; (ii) diretrizes para a investigação das condutas; (iii) geração de evidências digitais; e (iv) formas de colaboração internacional, como a extradição e a assistência jurídica recíproca. Recentemente, com a crescente e positiva incidência de novas leis sobre a proteção de dados pessoais ao redor do mundo, o debate sobre salvaguardas e proteção de dados no âmbito da segurança pública e da investigação criminal também ganhou destaque.

Contudo, a discussão não se limita apenas à harmonização das ações de investigação de crimes cibernéticos transnacionais. Uma parcela significativa das críticas dirigidas à Convenção é direcionada à criação de tipificações penais vagas e genéricas, onde a punição acaba sendo falha, tendo em vista a falta de proporcionalidade entre a conduta e o dano causado, tal como é o caso em comento.

No Brasil, a adesão à Convenção de Budapeste sobre o Crime Cibernético somente foi aprovada em dezembro de 2021. As discussões sobre o assunto têm se mostrado bastante frequentes no cenário atual, principalmente antes da aprovação de leis fundamentais no âmbito do legislativo brasileiro no cenário digital, como o Marco Civil da Internet, a Lei Geral de Proteção de Dados Pessoais e outras legislações correlatas que levaram a mudanças no Código Penal Brasileiro para incorporar

classificações de delitos cibernéticos. Durante a década de 2000, uma série de acontecimentos marcou o cenário mundial, sendo um deles, no país, um projeto de lei substitutivo a outros projetos de lei referentes a crimes na área digital apresentado pelo Senador Eduardo Azeredo (PL da Câmara nº 89, de 200361) que tentava promover, de maneira efetiva, algum nível de harmonização entre as tipificações e discussões presentes na Convenção de Budapeste contra o Cibercrime, buscando a devida proporcionalidade entre a conduta e as consequências geradas a partir dela.

Este texto foi fortemente contestado por organizações civis, ativistas e acadêmicos devido às tipificações genéricas e ambíguas que buscava inserir no sistema jurídico brasileiro. Em resposta, propôs-se uma legislação voltada para a defesa e a garantia de direitos no âmbito digital, culminando, em 2011, no envio de uma das primeiras versões do texto do Marco Civil da Internet para a Câmara dos Deputados.

No judiciário, um julgamento pelo Supremo Tribunal Federal (STF) decidiu acerca de uma controvérsia sobre o Acordo de Assistência Judiciário-Penal (MLAT), firmado entre Brasil e Estados Unidos. O STF decidiu que as autoridades brasileiras, incluindo o judiciário, podem solicitar diretamente às empresas de tecnologia estrangeiras dados e informações, eliminando assim os processos de cooperação jurídica internacional para a obtenção de conteúdos de aplicativos online localizados no exterior. Em 2020, o Supremo Tribunal Federal conduziu uma audiência pública para ouvir especialistas sobre o assunto, na qual foram mencionados diversos conceitos da Convenção de Budapeste, bem como a importância de respeitar os direitos humanos.

> **Decisão:** O Tribunal, por maioria, conheceu da ação declaratória de constitucionalidade, vencidos os Ministros André Mendonça e Nunes Marques. No mérito, por unanimidade, julgou parcialmente procedente o pedido formulado na inicial para declarar a constitucionalidade dos dispositivos indicados e da possibilidade de solicitação direta de dados e comunicações eletrônicas das autoridades nacionais a empresas de tecnologia, nas específicas hipóteses do art. 11 do Marco Civil da Internet e do art. 18 da Convenção de Budapeste, ou seja, nos casos de atividades de coleta e tratamento de dados no país, de posse ou controle dos dados por empresa com representação no Brasil e de crimes cometidos por indivíduos localizados em território nacional, com comunicação desta decisão ao Poder Legislativo e ao Poder Executivo, para que adotem as providências necessárias ao aperfeiçoamento do quadro legislativo, com a discussão e a aprovação do projeto da Lei Geral de Proteção de Dados para Fins Penais (LGPD Penal) e de novos acordos bilaterais ou multilaterais para a obtenção de dados e comunicações eletrônicas, como, por exemplo, a celebração do Acordo Executivo definido a partir do *Cloud Act*, tudo nos termos do voto do Relator.

> Ausentes, justificadamente, o Ministro Nunes Marques, que já havia proferido voto em assentada anterior, e o Ministro Roberto Barroso, que afirmou suspeição neste julgamento. Presidência da Ministra Rosa Weber. Plenário, 23.2.2023. (DECISÃO DO STF DA ADC 51, 2023).

Logo, ao analisar essa decisão levando em consideração o caso em comento, agora é possível fazer uma solicitação direta às empresas de tecnologia responsáveis por armazenar esses dados, em prol de uma busca efetiva pelos responsáveis pelos atos danosos, a fim de buscar a devida punição. No entanto, como já mencionado anteriormente no presente artigo, os crimes cometidos a partir de I.A. são de difícil detecção, diante da abrangência que são as redes de informação, assim como, sua acelerada disseminação pelas mídias sociais, tornando-se quase impossível identificar de onde veio a primeira postagem, tal como, o usuário que o publicou. Novamente, diante da vastidão de possibilidades que a internet oferece, sendo quase uma terra sem lei, é plenamente possível criar perfis fakes para fazer tais publicações e, em sua maioria, são perfis com o endereço de I.P (Internet Protocol) indetectáveis, impossibilitando seu rastreio.

E, foi exatamente isso que aconteceu com o caso concreto escolhido para o estudo, as imagens sensuais foram criadas a fim de prejudicar a Deputada e, na época dos fatos, candidata ao cargo do poder executivo da prefeitura de São Paulo. Com o objetivo único de manchar sua imagem perante a sociedade, prejudicando brutalmente sua campanha. Meses depois das publicações, o caso ainda se encontra sem solução, tendo em vista a dificuldade de rastrear os responsáveis pela produção e veiculação das imagens.

Diante do exposto, fica claro a deficiência quanto a um processo investigativo eficiente para trazer a resolução desse caso, assim como muitos outros semelhantes que até hoje encontram-se sem solução, restando somente os danos causados e as consequências irreparáveis. Não havendo uma retratação ou punição de fato e, como já apontado anteriormente, é extremamente difícil convencer a sociedade da inveracidade dos fatos inventados, podendo levar anos para que tal situação seja remediada. Logo, como ficam as vítimas? Devem somente rezar para haver algum descuido dos responsáveis diante das redes? E, em caso de não conseguir encontrar? Devem somente aceitar o dano causado e suas consequências? E quanto ao uso da imagem sem a devida autorização?

São tantas dúvidas que não são respondidas diante da incapacidade do sistema

investigatório, bem como, da omissão legislativa perante uma punição adequada e proporcional à conduta. Que, com a violação do direito fundamental que busca proteger a imagem, fica o questionamento sobre a insegurança jurídica e até onde a Constituição Federal pode proteger seus cidadãos e garantir os direitos fundamentais garantidos pela mesma.

E, apesar dos esforços pelo desenvolvimento da Convenção de Budapeste, ainda há muito o que considerar se quiserem ter um real controle sobre o uso indevido de tais ferramentas, como, por exemplo: com métodos investigativos efetivos, buscando um serviço especialista e qualificado próprio para essa área de atuação; uma regulação sobre os dados para as criações dessas contas indetectáveis, a fim de facilitar o rastreio; uma comissão internacional (levando em consideração as legislações e aspectos de cada país participante) visando elaborar estratégias punitivas que se adequam a proporcionalidade das condutas geradas a partir da utilização indevida dessas ferramentas.

6. CONCLUSÃO

Com base nas informações trazidas no presente artigo, o progresso acelerado das tecnologias de inteligência artificial, especialmente a aplicação de deep fakes, traz tanto possibilidades quanto desafios consideráveis para a sociedade atual. Contudo, conforme evidenciado no caso da Deputada Tabata Amaral, o uso malicioso dessas ferramentas destaca o grande potencial de prejuízo que a tecnologia pode causar quando usada de forma imprudente e ilegal. A produção e disseminação de conteúdos manipulados para difamar, desacreditar e ofender a honra de pessoas demonstram a vulnerabilidade do sistema legal brasileiro atual ao enfrentar esses novos tipos de delito digital. De acordo com Korshunov & Marcel (2019):

> "Com o avanço da tecnologia de deep fake, a criação de conteúdos alterados atingiu níveis tão sofisticados que se tornaram quase indistinguíveis da realidade para a maioria das pessoas. Isso gera um impacto significativo na confiança pública na veracidade de informações digitais, afetando desde interações cotidianas até processos eleitorais e judiciais. A precisão e a qualidade dos conteúdos adulterados aumentam o potencial de dano em esferas sociais, políticas e pessoais, enquanto dificultam sua detecção até mesmo por especialistas."

Logo, como já citado anteriormente, é de interesse público que as matérias que são veiculadas pelo país sejam revestidas de veracidade e disseminadas com responsabilidade, tendo em vista a grande repercussão e influência das mídias digitais, que tem o poder de persuadir a opinião pública.

Ainda, o artigo indica a inadequação das leis brasileiras específicas para tratar de crimes cibernéticos complexos, como os deep fakes. Embora leis como o Marco Civil da Internet, a Lei Geral de Proteção de Dados Pessoais e a Lei Carolina Dieckmann proporcionam orientações relevantes, elas são insuficientes para enfrentar a crescente complexidade tecnológica dos delitos cibernéticos. A falta de penalidades adequadas ou proporcionais ao efeito dos danos causados favorece um ambiente de impunidade, onde as vítimas frequentemente encontram obstáculos consideráveis para conseguir justiça ou remediar os danos sofridos.

A penalidade desses casos também é restringida pela dificuldade em identificar os autores das manipulações digitais, particularmente por causa do anonimato oferecido por redes sociais e outros canais digitais. Neste cenário, a situação de Tabata Amaral ilustra não só a infração ao direito básico de imagem, mas também o efeito psicológico e social que delitos desse tipo podem causar nas vítimas, sobretudo as mulheres, que são comumente submetidas a ataques que exploram sua sexualidade com o objetivo de humilhação e descrédito, onde a motivação é manchar a imagem e desmoralizar as vítimas.

Ademais, o texto reflete sobre a natureza abrangente deste problema. A utilização de deep fakes ultrapassa barreiras, tornando crucial a colaboração global para definir normas e práticas que minimizem os prejuízos ligados a essas ferramentas. Apesar de ser um marco significativo, a Convenção de Budapeste apresenta restrições ao ser implementada no Brasil, principalmente devido à escassez de infraestrutura para investigações eficientes e à falta de tipificações penais precisas para delitos cibernéticos avançados. A recente inclusão do Brasil na convenção é um avanço significativo, porém insuficiente diante da rapidez com que a tecnologia e os delitos relacionados se desenvolvem.

Portanto, é crucial sugerir soluções que incluam a regulamentação do uso de instrumentos de inteligência artificial, juntamente com a implementação de um sistema de investigação mais eficaz e especializado. É essencial capacitar profissionais para enfrentar crimes cibernéticos complexos, reforçar os mecanismos de detecção de

fraudes digitais e estabelecer uma responsabilidade conjunta entre os criadores de tecnologia e o governo. Ademais, é crucial promover discussões legislativas que levem à aprovação de leis específicas, como o Projeto de Lei nº 1272, que tem como objetivo criminalizar a alteração maliciosa de vídeos e áudios.

Um aspecto fundamental é a sensibilização da sociedade acerca dos perigos do uso desmedido de tecnologias de inteligência artificial. O estudo mencionado no artigo, que indica que 66% dos brasileiros não sabem o que é deep fake, evidencia a necessidade urgente de instruir a população para que ela se torne mais crítica e cautelosa na avaliação e propagação de informações digitais. A luta contra a desinformação deve ser uma prioridade, especialmente em um cenário onde a liberdade de expressão, mesmo sendo fundamental, não pode ser utilizada como justificativa para a disseminação de notícias falsas e ofensas à dignidade alheia. É de interesse público que essa visão crítica seja desenvolvida, pois a influência das mídias em relação à opinião pública está prejudicando vários campos do Estado Democrático de Direito, trazendo consequências severas com essa "chuva" de desinformação.

Em resumo, a análise do caso mostra como a tecnologia, quando não regulamentada e empregada de maneira ética, pode se transformar em um instrumento potente para infringir direitos básicos, arruinar reputações e provocar danos psicológicos irreparáveis. Contudo, ele também atua como um aviso e uma chance para que a sociedade, os legisladores e as entidades internacionais se unam na procura de soluções que fomentem a justiça e a segurança em um mundo progressivamente digital. Somente através de ações coordenadas será possível assegurar que os progressos tecnológicos sejam aplicados de forma ética, protegendo os direitos e a dignidade dos indivíduos, ao mesmo tempo que haverá o combate a práticas abusivas e criminosas.

REFERÊNCIAS

Hall, H. K. (2018). Deepfake videos: When seeing isn't believing**. Cath. UJL & Tech,** 27, 51. Disponível em: https://scholarship.law.edu/jlt/vol27/iss1/4 > Acesso em: 22 set. 2024.

KASPERSKY**. Mais de 65% dos brasileiros não sabem o que é "deepfake".** Disponível em: https://www.kaspersky.com.br/about/press-releases/62-dos-brasileiros-nao-sabem-re conhecer-uma-noticia-falsa > Acesso em: 23 set. 2024.

KORSHUNOV, P., & MARCEL, S. (2019, June). Vulnerability assessment and detection of

deepfake videos. In 2019 International Conference on Biometrics (ICB)(p. 1-6). **IEEE.** Disponível em: https://doi.org/10.1109/ICB45273.2019.8987375 > Acesso em: 21 set. 2024.

MENDONÇA, Helena C. F. Coelho; RODRIGUES, Paula Marques. **Deepfakenews e sua influência no universo feminino.** Migalhas, 4 jul. 2018. Disponível em: https://www.migalhas.com.br/dePeso/16,MI282987,31047-Deep+fake+news+e+sua+influencia+no+universo+feminino > Acesso em: 23 out. 2024.

MENEZES CORDEIRO, António. **Tratado de direito civil.** 4. ed. rev. e atual., com a colaboração de A. Barreto Menezes Cordeiro. Coimbra: Almedina, 2017. v. 4. p. 258.

O BRASIL E O MARCO CIVIL DA INTERNET. **Instituto Igarapé.** Disponível em: https://igarape.org.br/marcocivil/pt/. > Acesso em 23 out. 2024.

PORTAL G1**. Fato ou Fake?** Caso da Deputada Tabata Amaral**.** Disponível em: https://g1.globo.com/fato-ou-fake/sao-paulo/noticia/2024/09/15/e-fake-foto-de-tabata- amaral-em-pose-sensual-trata-se-de-deepfake.ghtml > Acesso em: 23 set. 2024.

PROJETO DE LEI N° 1272. **Adulteração maliciosa de vídeos ou áudios.** Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=9292780&disposition=inline> Acesso: 22 set. 2024.

ROMANO, Rafael Salomão. **O filme Rogue One: Uma História Star Wars e o direito de imagem. Consultor Jurídico, 29 dez. 2016.** Disponível em: https://www.conjur.com.br/2016-dez-29/rafael-salomao-romano-filme-rogue-onee-dire ito-imagem?imprimir=1 > Acesso em: 11 nov. 2024.

SAFERNET BRASIL. **PL sobre Crimes Cibernéticos:** Projeto de Lei Substitutivo do Senador Eduardo Azeredo (PSDB-MG). Disponível em: https://www.safernet.org.br/site/institucional/projetos/obsleg/pl-azeredo> Acesso em 06 nov. 2024.

SCOTT, DANIELLA. **"Deepfake Porn Nearly Ruined My Life",** Elle, 06 de fevereiro de 2020. Disponível em: https://www.elle.com/uk/life-and-culture/a30748079/deepfake-porn> Acesso: 21 set. 2024.

SENSITY TEAM. (2019). **Mapping the Deepfake Landscape. Sensity.** Disponível em: https://sensity.ai/blog/deepfake-detection/mapping-the-deepfake-landscape/> Acesso em: 23 set. 2024.

TRIBUNAL REGIONAL ELEITORAL DE MINAS GERAIS. **TRE-MG - MANDADO DE SEGURANÇA CÍVEL**: MSCiv XXXXX-47.2024.6.13.0000. UBERLÂNDIA– MG. 22/08/2024. Disponível em:https://www.jusbrasil.com.br/jurisprudencia/tre-mg/2678955979> Acesso em: 29 set. 2024.

VALE DA ESTRANHEZA. **Hipótese do vale da estranheza.** Disponível em: https://pt.wikipedia.org/wiki/Vale_da_estranheza > Acesso: 21 set. 2024.