ENSAIO SOBRE O USO DE DEEPPFAKE NO PROCESSO CRIMINAL: possíveis riscos e soluções

ESSAY ON THE USE OF DEEPPFAKES IN THE CRIMINAL PROCEDURE: possible risks and solutions

Pedro Enrico de Oliveira¹

Rafael Lima da Costa²

RESUMO

No direito processual penal, a adequada reconstrução dos fatos torna-se ainda mais relevante por atingir diretamente o direito fundamental à liberdade. Para tanto, a instrução processual deve ser realizada de modo eficiente e desprovida de deturpações que possam colocar em risco a idoneidade da prova obtida. Dentre os diversos meios de prova, as gravações em áudio e vídeo representam um dos elementos mais robustos de convencimento por possibilitarem um contato direto, por meio dos sentidos humanos, dos fatos tratados no processo judicial. Com o progresso da tecnologia computacional, notadamente da inteligência artificial e do aprendizado de máquina, surgem relevantes questionamentos sobre a idoneidade das gravações de áudio e vídeo como meios de prova, ante a capacidade de manipulação de seu conteúdo. A denominada deepfake permite a adulteração cada vez mais realista de seus elementos, com o objetivo de introduzir, retirar ou modificar as características originais. O objetivo desta pesquisa foi analisar os riscos ao processo penal pela difusão do uso de deepfakes e se há métodos eficazes para garantir a idoneidade das gravações em áudio e vídeo. Foi adotada abordagem qualitativa de revisão teórica. Como resultado, foi confirmada a existência de riscos ao processo penal pela popularização de aplicativos tecnológicos que facilitam a adulteração de gravações em áudio e vídeo. Para minimizar esses riscos, foram sugeridos métodos de checagem da originalidade dos arquivos e veracidade do conteúdo, para que a prova seja lícita.

Palavras-chave: Prova; Processo Penal; Deepfake; Inteligência artificial.

ABSTRACT

In the criminal procedural law, the adequate reconstruction of the facts becomes even more relevant because it directly affects the fundamental right to freedom. Therefore, the procedural instruction must be carried out efficiently and devoid of misrepresentations that may jeopardize the suitability of the evidence obtained. Among the various means of evidence, audio and video recordings represent one of the most robust elements of convincing as they allow direct contact, through human senses, to the facts dealt with in the judicial process. Through the improvement of computer technology, notably the artificial intelligence and machine learning, relevant

¹ Mestrando Profissional em Direito e Poder Judiciário pela Escola Nacional de Formação e Aperfeiçoamento de Magistrados, Especialista em Direito Processual Civil, Especialista em Direitos Humanos, Teoria e Filosofia do Direito, Juiz de Direito do Tribunal de Justiça do Estado do Pará.

² Mestrando Profissional em Direito e Poder Judiciário pela Escola Nacional de Formação e Aperfeiçoamento de Magistrados, Especialista em Direito Processual Civil, Especialista em Direito Administrativo, Juiz Federal do Tribunal Regional Federal da 1ª Região.

questions arise about the suitability of audio and video recordings as evidence, given the ability to manipulate their content. The so-called deepfake allows for the increasingly realistic tampering of its elements, with the aim of introducing, removing or modifying the original characteristics. The objective of this research was to analyze the risks to the criminal procedure on the diffusion of the use of deepfakes and whether there are effective methods to guarantee the suitability of audio and video recordings. A qualitative theoretical review approach was adopted. As a result, the existence of risks to criminal procedure was confirmed by the popularization of technological applications that facilitate the tampering of audio and video recordings. To minimize these risks, methods were suggested to check the originality of the files and the veracity of the content, so that the evidence is lawful.

Keywords: Evidence; Criminal Procedure; Deepfake; Artificial Intelligence.

1 INTRODUÇÃO

O Poder Judiciário vem passando por um processo de virtualização de suas atividades, com o escopo de aumentar sua eficiência. A adoção do processo eletrônico acarreta em uma modificação relevante na forma como os atos processuais são praticados, repercutindo na própria produção probatória.

No âmbito do processo penal, em que deve ser conferido máximo respeito ao direito constitucional à ampla defesa, apresenta-se relevante a análise da prova introduzida no processo eletrônico. Ao ser transmudada ou produzida com natureza digital, a prova passa a ser integrada à dinâmica do ambiente da tecnologia da informação, o que inclui a possível influência da inteligência artificial.

Tendo por base esses aspectos, realizou-se o presente estudo com o objetivo de responder os seguintes problemas: existem riscos à higidez do processo penal, atuais ou potenciais, decorrentes da utilização da prova digital? A inteligência artificial é capaz de adulterar o conteúdo da prova de maneira a influenciar indevidamente a formação da convicção do julgador no processo penal? Existem métodos ou ferramentas para a gestão adequada de riscos relacionados a valoração da prova digital no processo penal?

A pesquisa teórica justifica-se pela difusão de ferramentas tecnológicas que tem a aptidão de manipular imagens e áudios, com a inserção, retirada ou adulteração de elementos que alteram por completo a mensagem original ou modificam de forma imperceptível o seu emissor, o que passou a ser conhecido como *deepfake*.

Quando tais materiais passam a ser valorados como elementos de prova em processo judicial que tem a liberdade como um dos bens jurídicos em análise, torna-se relevante discutir métodos e mecanismos para reconhecer essa manipulação e extirpá-la do processo.

A hipótese central defendida por este artigo é a de que o atual estágio de desenvolvimento da tecnologia da informação e, mais especificamente, da

inteligência artificial, já tem o condão de gerar riscos à autenticidade e integridade da prova digital inserida no processo eletrônico. Assim, é necessário que seja criada estrutura integrada ao Poder Judiciário para a prevenção desses riscos, com investimentos em equipes especializadas na detecção da chamada *deepfake* e uso da própria inteligência artificial como ferramenta de identificação dessa manipulação de dados.

Desenvolveu-se a pesquisa com a coleta de dados em revisão teórica, que foram analisados pelo método qualitativo. Abordou-se o tema com uma visão multidisciplinar do Direito e da ciência da computação.

O artigo foi dividido em quatro seções, sendo a primeira a introdução. A segunda seção consiste na moldura conceitual e teórica da pesquisa. Nela, foram analisados aspectos relacionados à garantia dos direitos fundamentais no processo penal ante a virtualização do Poder Judiciário, bem como foi abordada a prova digital como categoria específica passível de sofrer ingerência da tecnologia da informação. A terceira seção traz análise da utilização da inteligência artificial como instrumento para a adulteração de dados inseridos em gravações de áudio e vídeo, o que se denomina de *deepfake*, e a capacidade que estes conteúdos têm de influir no resultado do processo penal. Também são sugeridos métodos e ferramentas para o controle do material inserido no processo penal, com o objetivo de identificar eventuais manipulações. Por fim, a quarta seção traz as conclusões desta pesquisa.

2 MOLDURA CONCEITUAL E TEÓRICA

2.1 A VIRTUALIZAÇÃO DO PODER JUDICIÁRIO E O EXERCÍCIO DO DIREITO DE DEFESA

O ambiente virtual tem por característica a perda de uma base territorial, havendo verdadeira separação do espaço geográfico e da unidade de tempo como costuma ser medida (LÉVY, 2011). O Poder Judiciário na busca por melhoria em sua eficiência vem adotando medidas para alterar a forma de sua atuação, passando de uma tradição solene, lastreada em atos presenciais e numa estrutura física, para o ambiente dinâmico e flexível possibilitado pela tecnologia computacional conectada em rede.

A Lei nº 11.419 de 2006 autorizou de forma expressa a utilização de meio eletrônico para a tramitação de processos judiciais, comunicação de atos e transmissão de peças processuais. Ainda que já existisse a Lei nº 9.800 de 1999, que autorizava de forma genérica às partes o envio de petições escritas por meio de sistema de transmissão de dados, pode-se na Lei nº 11.419/2006 o marco

introdutório do processo eletrônico no Brasil, em razão de sua amplitude e conformação.

Mallmann (2016) destaca que antes do próprio advento da Lei nº 11.419/2006, o Tribunal Regional Federal da 4ª Região, por meio da Resolução nº 13/2004, estabeleceu que com a implantação de sistema de processamento de demandas em âmbito eletrônico (e-proc), as ações deveriam ser ajuizadas por meio desse sistema.

Atualmente, todos os Tribunais brasileiros utilizam sistemas de processamento eletrônico de feitos, o que faz com que a produção probatória ocorra de forma preponderante em âmbito digital. De acordo com o Relatório Justiça em Números (CONSELHO NACIONAL DE JUSTIÇA, 2021), em 2020, apenas 3,1% do total de novos processos tiveram ingresso físico no Poder Judiciário, o que possibilitou fosse alcançado o percentual de adesão ao processo eletrônico de 96,9% da totalidade de processos em tramitação, seja por meio da utilização do Processo Judicial Eletrônico (PJE) ou outros sistemas eletrônicos, conforme autorização da Resolução 185/2013, do CNJ. Merece destaque que 48 tribunais alcançaram 100% de processos eletrônicos³.

Um dos aspectos positivos relacionados à consolidação do processo eletrônico é a possibilidade de encurtamento do tempo do processo, considerando que a morosidade gera problemas de acesso à justiça, afastando do sistema de Justiça os detentores de legítimo interesse (GICO JR., 2015). A grande quantidade de demandas existentes no Poder Judiciário é o principal motivo dessa morosidade. Consoante consta do Relatório Justiça em Números (CONSELHO NACIONAL DE JUSTIÇA, 2021), ao término do ano de 2020 havia no Brasil 74,5 milhões de processos pendentes de solução definitiva, para um universo de 17.988 magistrados.

No âmbito do direito processual penal a preocupação com a celeridade processual deve ser analisada com parcimônia, uma vez que o bem jurídico diretamente tratado é a liberdade. Tão importante quanto à efetiva entrega da tutela jurisdicional é, portanto, o respeito ao devido processo garantido constitucionalmente, devendo ser oportunizado ao acusado todo o tempo que for realmente necessário ao exercício do direito fundamental à ampla defesa.

Mas isso não significa que não devam ser adotados instrumentos mais céleres para a prática dos atos processuais, com a utilização dos meios tecnológicos disponíveis, desde que autorizados normativamente. Isso já ocorre com as audiências, inclusive de instrução e julgamento, nas quais é admitido o uso de

3 TJPR, TJGO, TJDFT, TJSC, TJAP, TJTO, TJMS, TJAM, TJAL, TJAC, TJSE, TRE-BA, TRE-RS, TRE-SP, TRE-PR, TRE-RJ, TRE-MG, TRE-MA, TRE-SC, TRE-MT, TRE-GO, TRE-PI, TRE-PE, TRE-PB, TRE-CE, TRE-RO, TRE-RN, TRE-DF, TRE-AL, TRE-TO, TRE-AM, TRE-AC, TRT15, TRT4, TRT9, TRT18, TRT7, TRT23, TRT16, TRT13, TRT11, TRT24, TRT14, TST, STM, TRF4, TRF5 e TJRS

videoconferência para a oitiva de testemunhas e colheita do interrogatório do réu (artigo 185, §2º e artigo 222, §3º, ambos do Código de Processo Penal).

Quando o meio tecnológico pode causar algum tipo de risco à finalidade do ato ou a direito fundamental do réu, a legislação proíbe sua realização, como ocorre com a vedação expressa à realização de audiência por videoconferência para as audiências de custódia, conforme previsto no art. 3º-B, §1º, introduzido pela lei nº 13.964, de 2019.

O respeito ao procedimento é forma de proteger não apenas o acusado, mas toda a sociedade, ao se manter hígido o ordenamento jurídico. Assim, a flexibilização de formalidades, com o argumento de melhorar a eficiência do sistema de Justiça, pode representar verdadeiro risco a direitos fundamentais, uma vez que o procedimento tem também por finalidade a redução de assimetrias de poder (CABRAL, 2010).

O direito processual penal é o instrumento utilizado para a aplicação das normas materiais de direito penal, sendo formal e solene como garantia ao devido processo previsto constitucionalmente. O escopo é a reconstrução histórica dos fatos da forma mais próxima da realidade com a finalidade de auxiliar na formação do convencimento do julgador.

A verdade deve, pois, ser transposta para dentro do processo judicial. Como bem aponta Oliveira (2005), apesar de a verdade ser um elemento essencial para o correto exercício da jurisdição penal, ela é de difícil alcance. Não basta que se saiba de sua existência, é necessário que os elementos que a evidencie sejam instrumentalizados de modo a garantir a confrontação pela parte interessada, em um legítimo exercício do contraditório e da ampla defesa. Os fatos alegados devem, portanto, ser provados para que possam ser levados em consideração em um processo judicial legítimo.

2.2 A PRODUÇÃO PROBATÓRIA E O PROCESSO ELETRÔNICO

Prova é vocábulo polissêmico no âmbito do Direito, uma vez que consiste no processo de aferição da correspondência de uma alegação com a realidade, mas também é utilizado como designação dos meios que são admitidos para que essa realidade seja verificada formalmente. Representa, ainda, o resultado do processo de verificação da alegação (NUCCI, 2007).

Realizando uma distinção entre meios de prova, meios de obtenção de prova e fonte de prova Távora e Alencar (2016) esclarecem que os meios de prova são os instrumentos que possibilitam a inserção no processo de elementos em linguagem compatível com ele. Já os meios de obtenção de prova são normalmente

extraprocessuais, tendo por escopo encontrar fontes de prova ou seus elementos materiais, como ocorre em uma interceptação telefônica. Os referidos autores destacam, ainda, que fonte de prova é a pessoa ou coisa de onde emana a prova. Também fazem referência a técnicas especiais de investigação, como a colaboração premiada, interceptação telefônica, dentre outras.

O ordenamento jurídico brasileiro especifica algumas espécies de prova. Todavia, não há exclusividade quanto às provas nominadas, sendo admitidos todos os elementos de prova que tenham o condão de demonstrar a ocorrência de determinado fato relevante para o processo judicial, ainda que não estejam expressamente previstas em lei, mas desde que estejam em consonância com esse ordenamento jurídico.

De forma mais simplificada, as provas podem ser divididas em três categorias básicas, que seriam a prova testemunhal, a prova documental e a prova pericial (VAZ, 2012). Atualmente todas essas categorias podem utilizar instrumentos tecnológicos para serem produzidas, o que aumenta a preocupação quanto à autenticidade de seu conteúdo.

Como é cediço, os meios de obtenção da prova devem ser lícitos para que ela seja aceita como elemento de formação da convicção do julgador em um processo judicial. Essa previsão encontra guarida expressa no art. 5º, LVI da Constituição Federal. O Código de Processo Penal em seu art. 157 também apresenta vedação quanto à utilização de provas obtidas com violação às regras constitucionais e legais. A ilicitude alcança outras provas que tenham sido derivadas de provas obtidas por meios ilícitos, ou seja, quando não tiverem sido obtidas por uma fonte independente.

De acordo com o art. 157, §5º, do Código de Processo Penal, introduzido pela Lei nº 13.964/2019, o próprio magistrado que tiver contato direto com a prova reconhecida como ilícita deve ser afastado do julgamento da causa, como forma de garantir a higidez do processo judicial.

Essa é uma preocupação relacionada com os meios de obtenção da prova. Todavia, com o desenvolvimento de ferramentas tecnológicas cada vez mais modernas, o cuidado não somente com os meios de obtenção da prova, mas com o seu próprio conteúdo passou a ser extremamente relevante.

O conceito de prova, suas características e limites, mesmo no processo penal, devem se adequar à evolução da sociedade e, notadamente, ao desenvolvimento tecnológico, que acaba por criar diversas outras formas de apreensão da realidade fática. Sempre deve haver, todavia o respeito aos direitos fundamentais dos envolvidos.

Tradicionalmente, a prova era documentalmente inserida nos autos físicos do

processo judicial. Mesmo a prova oral costumava ter seu conteúdo reduzido formalmente a termo, com a assinatura dos participantes para a legitimação da prova produzida. Com o advento e difusão dos sistemas de gravação em áudio e vídeo, o próprio Poder Judiciário passou a introduzir diretamente nos autos mídias com o conteúdo das audiências realizadas em juízo, o que favoreceu o contato direto com a prova.

A prova material, que é aquela que está diretamente relacionada à demonstração de um fato, como um exame de corpo de delito e a documental, que condensa graficamente a manifestação de um pensamento (TÁVORA; ALENCAR, 2016) passam por um processo de digitalização para que possam ser inseridas no processo eletrônico.

Com a preponderância do processo eletrônico, mesmo áudios e vídeos gravados inicialmente em formato analógico deverão ser convertidos para o formato digital, consistindo na utilização de tecnologia computacional para adoção do sistema binário, que é um sistema posicional de numeração, com emprego dos dígitos 1 e 0, baseado na álgebra de Boole (VIDAL; SANTOS; NOGUEIRA, 2016).

Além dessas provas que seriam originalmente físicas, constata-se a profusão de documentos digitais que são aqueles documentos gerados diretamente no ambiente digital ou que foram inseridos em um suporte digital antes de serem apreendidos em uma investigação criminal ou na instrução processual e que podem ser utilizados como elemento probatório.

Como bem esclarece Vaz (2012) a prova digital, vista como fonte real, pode consistir no suporte no qual estão armazenados dados, tais como computadores, pen drives CD's, DVD's, celulares, câmeras de vídeo ou fotográficas. Também aduz que são fontes reais as próprias imagens, vídeos, músicas, documentos de texto, dentre outros.

A prova digital consistiria, então, nos dados que estão em suporte eletrônico ou que são transmitidos por uma rede de comunicação como a internet e que estão em um formato digital, representando fatos ou ideias (VAZ, 2012).

A referida autora aponta como principal característica da prova digital o fato de se tratar de um objeto imaterial, uma vez que consiste em uma sequência numérica e que, por essa razão, tem a facilidade de ser alterado, bem como pode ser copiado e difundido, sendo necessário um equipamento intermediário para seu acesso.

A adoção de métodos de gestão dos riscos relacionados à utilização da prova digital é imprescindível para a garantia da validade do processo penal. Não é recomendável que a autenticidade desse tipo de prova seja aferida apenas quando houver alegação da parte contrária, uma vez que a consolidação do processo

eletrônico depende do reconhecimento de que ele é seguro e capaz de preservar os direitos fundamentais.

Para fins de exemplificação da quantidade de elementos probatórios digitais que atualmente são apreendidos em operações policiais de maior envergadura, de acordo com dados extraídos do sítio eletrônico oficial da Polícia Federal (POLÍCIA FEDERAL. MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA, 2018), relativos à chamada operação lava-jato, até o dia 14/08/2017, haviam sido apreendidos e submetidos à perícia 5.754 elementos de prova.

A maior parte desses elementos foram obtidos a partir de dispositivos de armazenamento e equipamentos computacionais, quais sejam, 1.592 *pendrives* (28%); 985 discos rígidos de computador (17%); 967 telefones celulares (17%); 725 computadores (13%); 437 mídias óticas (8%); 139 cartões de memória (2%); 100 disquetes (2%); 97 *tablets* (2%); 93 CD's (2%); 77 DVD's (1%); 25 fitas magnéticas (1%); 14 cartões SIM (0,5%); 128 outros dispositivos computacionais (2%); 74 outros dispositivos de armazenamento computacional (1%). Constata-se que 68,5% de todo o material apreendido corresponde a aparelhos de onde são extraídos dados digitais ou digitalizados.

Assim, é necessário sejam observados pressupostos de validade e utilidade dessa prova digital. Como bem delineado por THAMAY e TAMER (2020), a prova digital somente será útil ao seu propósito se for autêntica, íntegra e respeitar a cadeia de custódia.

Pontuam os autores que a autenticidade consiste na possibilidade de se atestar a autoria do fato digital. Não pode haver, assim, qualquer dúvida sobre quem foi o responsável pela constituição do fato no meio digital ou dele participou.

Sobre esse aspecto, importante mencionar as previsões normativas existentes que buscam garantir a autenticidade de documentos que são utilizados como elementos de prova. A Medida Provisória nº 2.200, de 2001, que trata sobre a Infraestrutura de Chaves Públicas Brasileiras – IC–Brasil, tem por escopo exatamente garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica. De igual modo, o art. 19 do Código de Processo Civil possibilita pedido de declaração sobre a autenticidade de documento.

No âmbito do processo penal diversas são as normas que abordam a necessidade de garantia da autenticidade do documento, sob pena de nulidade do ato, como o previsto nos artigos 39, 166, 174, II, 232, 235, 289, §2º, 289-A, §2º, 299, 541, §§1º e 2º, 543, II, 782, 788, IV e 789, §4º, todos do Código de Processo Penal. Também há referência à garantia da autenticidade na Consolidação das Leis Trabalhistas, na própria lei que trata sobre o processo eletrônico (art.12 da Lei nº 11.419/2006) e no art. 2º do Decreto nº 10.046, de 2019, que disciplina a governança

no compartilhamento de dados no âmbito da Administração Pública (THAMAY; TAMER, 2020).

Outro pressuposto para a utilidade da prova digital e que está diretamente relacionado com o objeto do presente estudo é a integridade do conteúdo. Conforme esclarecido por Thamay e Tamer (2020), a integridade diz respeito à ausência de modificação em seu estado ou adulteração, a partir da realização do fato que consiste na fonte da prova digital até a apresentação do seu resultado. Ou seja, deve haver uma correspondência integral dos elementos fáticos desde a sua apreensão do mundo real e sua inserção em um ambiente digital até o momento em que esse conteúdo é apreciado pelo observador.

Deve haver, portanto, uma preocupação com a formalidade de identificação e resguardo do suporte eletrônico no qual constam os dados que representam a fonte da prova a ser levada em consideração em um processo judicial. Havendo dúvidas quanto a integridade do elemento de prova ele deve ser descartado, ante a aplicação do princípio *in dubio pro reo*.

A integridade e a autenticidade da prova estão intrinsecamente ligadas a sua cadeia de custódia, que é o registro histórico, acompanhável por qualquer pessoa autorizada, que evidencie todo o transcurso desde sua captação até sua apreciação (THAMAY; TAMER, 2020). A previsão legal sobre a necessidade de observância da cadeia de custódia foi estabelecida pela Lei nº 13.964/2019, denominada de Pacote Anticrime, a qual introduziu no Código de Processo Penal o artigo 158-A.

Com o avanço da tecnologia da informação, notadamente da inteligência artificial e a sua capacidade de manipulação de elementos inseridos no ambiente digital e a consolidação do processo eletrônico, que passa a exigir que toda prova produzida tramite de forma digital, surge a séria preocupação com esses três pressupostos para a utilidade desse tipo de prova.

Passa-se, então, a abordar especificamente o problema relacionado à manipulação de imagens de vídeo por meio do emprego de tecnologia computacional, o que passou a ser denominado de *deepfake* e como isso pode impactar na higidez da produção probatória no processo penal.

2.3 OS IMPACTOS DA INTELIGÊNCIA ARTIFICIAL NA VALORAÇÃO DA PROVA

A inteligência artificial vem sendo utilizada em diversos ramos da sociedade como forma de facilitar as atividades desempenhadas pelos seres humanos, de modo que sua aplicação também é útil para os serviços prestados pelo Poder Judiciário.

Pedrina (2019) apresenta três questionamentos relevantes sobre a aplicação

da inteligência artificial no âmbito das atividades judiciárias, mais especificamente no processo penal. O primeiro deles está relacionado diretamente à capacidade de uma máquina substituir o julgador humano. O segundo diz respeito à aferição da viabilidade de a tecnologia atualmente existente ser adotada na esfera do processo penal ou de ter o condão de influir nessa seara, e, por fim, quais seriam as perspectivas para o futuro.

Atualmente o ato de julgar não pode ser integralmente realizado pela inteligência artificial, principalmente por meio da aplicação apenas da computação estatística, ante a complexidade dessa atividade. Por outro lado, é inegável que a inteligência artificial já vem influenciando no âmbito das atividades do Poder Judiciário e do próprio processo judicial, com perspectiva de aprofundamento dessa influência, com consequências positivas, mas também possíveis consequências negativas.

Para Pedrina (2019) a tecnologia de inteligência artificial atualmente existente pode ser útil ao processo penal para a aplicação de teses em tribunais, tendo por base a leitura automática dos processos, com a utilização da tecnologia OCR - *Optical Character Recognition* (Reconhecimento Ótico de Caracteres). Também pode ser utilizado para aplicação de standards probatórios, como, por exemplo, na recomendação para o reconhecimento do delito de tráfico de drogas, a depender da quantidade de entorpecente apreendida. Outras utilidades apontadas seriam o uso para a busca de evidências já existentes nos autos e elaboração de perguntas em auxílio ao julgador.

Por outro lado, a inteligência artificial pode ser utilizada pelos sujeitos processuais ou por terceiros com a finalidade específica de deturpar o devido processo legal, com mecanismos como, por exemplo, o a adulteração das provas, que, conforme já exposto, passam a ser produzidas ou analisadas em um ambiente digital ao serem inseridas no processo judicial eletrônico, tornando-as mais suscetíveis de modificação.

2.3.1 O que são *deepfakes*

Uma *deepfake* é um vídeo hiper-realista que aplica inteligência artificial (IA) para retratar alguém dizendo e fazendo coisas que nunca aconteceu (Westerlund, 2019). Usualmente, são utilizadas redes neurais artificiais para analisar um grande conjunto de amostra de dados para produzir o conteúdo digital que imite as expressões faciais, voz e características da face humana.

O vernáculo *deepfake* é um neologismo da língua inglesa que combina o *deep learning* (aprendizado profundo de máquina) com o predicado *fake* (falso), indicando que *deepfake* é um conteúdo digital produzido e falseado por modelo de

inteligência artificial, normalmente, por aplicação de aprendizado profundo de máquina, que realiza a fusão, a combinação, a substituição e a sobreposição de imagens e vídeos, criando um conteúdo falso. Uma vez alimentado o algoritmo com a imagem necessária, o vídeo falso com o conteúdo de áudio é criado (MARAS e ALEXANDROU, 2019).

O principal atributo de uma *deepfake* é o de deixar poucos vestígios de manipulação e, como consequência, a verificação da realidade se torna extremamente difícil do ponto de vista humano ou tecnológico. No ano de 2019, o professor Hao Li, pioneiro no desenvolvimento de algoritmos de *deepfake*, expressava inquietação sobre a velocidade do avanço deste tipo de tecnologia e afirmou que em dois ou três anos uma *deepfake* seria perfeita e que não haveria como dizer se era real ou não (O'NEILL, 2019).

Para compreender o por que desta inquietação exposta por um dos mais respeitados cientistas da computação no mundo, é necessário compreender como o modelo de inteligência artificial gera uma *deepfake*.

Inteligência artificial não possui um conceito dogmático completo e acabado. Russel e Norvig (2016), em literatura clássica sobre o tema, optaram por não atribuir um conceito à IA, senão, em separar dois grupos conceituais, de acordo com a forma de execução: IA como o processo de pensamento e raciocínio, e a IA como comportamento (ação). Verificaram, também, que as formas de execução são mensuradas pela sua capacidade de reproduzir com fidelidade a performance humana (pensam ou agem humanamente), ou de desempenhar uma métrica ideal (pensam ou agem racionalmente).

Os modelos computacionais mais sofisticados e complexos não produzem respostas lineares e binárias. Modelos que processam linguagem natural ou reconhecem fala e imagens, por exemplo, sustentam grande parte de suas capacidades de processar dados na neurociência, emulando artificialmente as redes neurais biológicas que compõem o sistema nervoso humano. Os dados são inseridos no modelo e distribuídos em diversas camadas (layers), onde são atribuídos pesos diferentes, produzindo uma resposta coerente com o treinamento recebido.

Os modelos que produzem *deepfake*, frequentemente, utilizam redes neurais ou o aprendizado profundo de máquina. Estas abordagens de inteligência artificial produzem respostas melhores não pela forma como são treinados, mas, pela qualidade e quantidade de dados inseridos. Quanto mais dados são inseridos, mais o modelo aprende e mais aperfeiçoada fica a resposta gerada. Isto significa que, quanto mais dados de expressões faciais, gestos humanos característicos, idiosincrasias e tipos vocais são inseridos no modelo, mais aperfeiçoado é o vídeo (imagem e áudio) produzido, ou seja, mais real se parece aquilo que é falso.

Wiggers (2019) explica que muitos modelos de inteligência artificial para a geração de *deepfakes* são desenvolvidos por uma abordagem chamada de GANs (*generative adversarial networks*, ou redes adversárias generativas). Este método de inteligência artificial utiliza dois algoritmos de forma adversarial, sendo um com a atribuição de gerar e o outro de discriminar (julgar) o que foi gerado pelo primeiro. Assim, são inseridos os dados reais em ambos os modelos e, enquanto um, valendo-se da base de dados real, gera uma amostra falsa, o outro tenta diferenciar qual é a amostra real e qual é a falsa. Após o resultado, o algoritmo discriminador relaciona os erros e os acertos do algoritmo gerador, que, então, aprende com os seus próprios erros e acertos.

Com o tempo, o gerador melhora a sua saída e o discriminador melhora a detecção das amostras falsas. Um algoritmo retroalimenta o outro.

Ou seja, quanto mais aperfeiçoada é a resposta produzida pelo modelo, mais difícil é a detecção do falseamento pelo ser humano ou por outra ferramenta tecnológica.

Acerca do uso desta tecnologia, Westerlund (2019) alerta que, embora os primeiros exemplos de *deepfakes* se concentrassem em questões políticas, líderes, atrizes, comediantes e artistas tendo seus rostos transformados em vídeos pornôis (*apud* HASAN e SALAH, 2019), *deepfakes* no futuro serão mais e mais usados para pornografia de vingança, *bullying*, uso de vídeo falso como prova em tribunais, sabotagem política, propaganda terrorista, chantagem, manipulação de mercado e falsificação de notícias (*apud* MARAS e ALEXANDROU, 2019).

Softwares para a criação de *deepfakes* estão disponíveis gratuitamente para qualquer usuário de tecnologia comum, ou seja, qualquer cidadão possui condições de produzir vídeos, áudios e imagens falsas, o que torna a questão ainda mais desafiante do ponto de vista regulatório e de controle.

2.3.2 *Deepfake* como elemento de prova e como conteúdo de desinformação

No que importa ao processo penal, é importante destacar que uma *deepfake* pode, a um só tempo, ser usada como elemento de prova e gerar desinformação (*misinformation*) para influir na sensibilidade do julgador, seja o juiz singular, ou um corpo colegiado, como no caso dos jurados do tribunal do júri.

Farid (2021) discute que a imortalidade digital pode ser ou não desejável. É desejável, por exemplo, que relatórios de violações de direitos humanos e corrupção corporativa permaneçam como parte do registro público. Contudo, conteúdos de terror digital, abuso sexual infantil, imagens íntimas não consensuais e desinformação perigosa não deveriam ser encontrados facilmente no mundo online.

No caso das *deepfakes* e outros conteúdos digitais falsos, quando relacionados à prática de algum crime, podem influenciar a opinião pública e alterar a capacidade de isenção na análise de provas reais pelo juiz no julgamento do processo penal (v.g., a decisão tomada por jurados em uma sessão de Tribunal do Júri, no julgamento de crimes dolosos contra a vida). Ocorre que, segundo Farid (2021), nem a própria inteligência artificial ou a moderação humana são capazes de lidar com a disseminação de conteúdo nocivo.

A era da informação, que é marcada pela massiva quantidade de dados a que as pessoas estão sujeitas, também se tornou a era da desinformação (*fake news*), pois substancial parte desses dados não corresponde à realidade. As pessoas atribuem grande peso probatório a imagens e vídeos (PFEFFERKORN, 2020) e, neste ponto, a análise da prova contida em vídeos acaba possuindo mão dupla: na era da informação e da desinformação, uma *deepfake* apresentada como prova pode gerar certeza no julgador, enquanto uma prova legítima pode ser vista com dúvida. Acredita-se no falso e duvida-se do real.

3 DISCUSSÃO QUALITATIVA

O desenvolvimento tecnológico agrava os riscos inerentes à vida em comunidade, uma vez que a conduta humana passa a ser um elemento relevante na geração de insegurança e perigos (BECK, 2011). Já foi demonstrado que a utilização da tecnologia da informação e da inteligência artificial na manipulação de sons e imagens gera riscos relevantes para a validade da instrução processual no processo penal.

Para minimizar esses riscos, impõem-se perquirir sobre a existência de métodos de gestão e instrumentos eficazes na identificação e tratamento desses dados fraudulentamente criados e inseridos em um processo judicial eletrônico.

Merece destaque o fato de esta preocupação estar difundida por todo o mundo, uma vez que a utilização de *deepfake* impacta não apenas o processo penal, objeto do presente estudo, mas o processo democrático, as relações intergovernamentais e empresariais, e, principalmente, atinge a imagem e intimidade de qualquer pessoa. Por essa razão, empresas ligadas à internet e redes sociais estão buscando combater o conteúdo falso (*fake news*), que passa a ser mais realista e com maior potencial de enganar quando utiliza a inteligência artificial para criar a *deepfake*.

A empresa Google, no ano de 2018, apresentou uma iniciativa ao custo de 300 milhões de dólares para combater a desinformação gerada ou divulgada na internet (HALL, 2018). Um dos aspectos interessantes dessa iniciativa foi a criação

de redes de checagem de fatos, com a divulgação de informações detalhadas sobre as fontes das mensagens difundidas e a introdução do Google News Initiative (GNI), que consiste em um laboratório para enfrentamento da desinformação. A rede social Facebook, recentemente renomeado para Meta, também estaria adotando mecanismos para combater a desinformação divulgada pela internet. Mesmo a companhia defendendo o direito à liberdade de expressão, sua porta-voz, Lauren Svensson, reconheceu ser necessário retirar a relevância de conteúdo inautêntico, sendo um dos caminhos a desmonetização desse tipo de conteúdo (HALL, 2018).

O controle da informação por órgãos governamentais costuma receber críticas embasadas no risco à liberdade de expressão que essa atuação poderia causar, o que já ocorre em países com menor abertura democrática, como a China. Neste país, o governo controla boa parte do acesso à informação, de sorte que os cidadãos têm apenas um direito implícito a ele, que está sujeito à comprovação da necessidade, tendo, ainda assim, uma esfera muito limitada. Toda informação que possa trazer algum prejuízo à segurança estatal, segurança pública, segurança econômica ou a estabilidade social estão excluídas do acesso por cidadãos (XIAO, 2015). Por serem conceitos extremamente vagos e analisados por quem presta a informação, conclui-se que o direito ao acesso à informação existe apenas formalmente.

Se o controle da informação de forma genérica e ampla por órgãos governamentais pode trazer riscos, a ausência de controle do conteúdo dessa informação também traz riscos graves à sociedade, notadamente quando esses elementos são utilizados pelo próprio Estado no exercício de uma de suas atividades mais impactantes na vida das pessoas que é a jurisdição.

Portanto, denota-se que o combate ao uso de *deepfakes* no processo criminal não pode ser realizado somente no âmbito do processo. Westerlund (2019) sugere que sejam combatidas por meio de legislação e regulamentação, políticas corporativas e ações voluntárias, educação e treinamento, bem como pelo desenvolvimento de tecnologia para detecção de *deepfake*, autenticação de conteúdo e prevenção.

As sugestões que seguirão pretendem ser apenas uma modesta contribuição para a comunidade científica.

3.1 PROPOSTAS E DESAFIOS PARA O ENFRENTAMENTO DA *DEEPPFAKE* NO PROCESSO PENAL

Garantia da autenticidade, a integridade deve ser a regra para a utilização da prova digital, o que inclui os documentos que contenham gravações em áudio e

vídeo. Para tanto, não se pode afastar da perícia técnica, que normalmente é utilizada com a finalidade de conferir respaldo técnico ao julgador quanto a elementos fáticos que necessitam da posição de um especialista, conforme já previsto no art. 158 e seguintes do Código de Processo Penal.

A própria metodologia de perícia técnica para casos que envolvam a utilização de *deepfake* deve ser readequado, buscando maior integração e dinamismo compatíveis com a fluidez em que se desenvolve a tecnologia da informação e a inteligência artificial.

A perícia técnica deve possuir como método a padronização de procedimentos e a estruturação dos laboratórios forenses com controles internos de qualidade e equipamentos tecnológicos eficazes para a realização dos exames (GIOVANELLI; GARRIDO, 2011) .

A criação de órgãos integrantes do Poder Judiciário que tenham por finalidade realizar a apreciação da autenticidade e integridade da prova digital, o que inclui as gravações e áudio e vídeo, pode se tornar tão necessária quanto os demais órgãos administrativos de apoio, tais como núcleos de contadoria judicial ou de cumprimento de atos judiciais. Como já exposto, ao estruturar praticamente toda a sua atuação em ambiente eletrônico, o Poder Judiciário passa a ter a obrigação de garantir que esse ambiente é seguro, gerando a credibilidade necessária para sua consolidação.

Considerando que a prova digital não guarda limites territoriais, bem como é de fácil transmissão, a estrutura para a realização das perícias técnicas sobre a fonte da prova pode ser centralizada ou, ainda que regionalizada, ser integrada em rede de colaboração pelos diversos órgãos que compõem o Poder Judiciário.

Para tanto, entende-se que o Conselho Nacional de Justiça (CNJ), como órgão responsável pelo controle da atuação administrativa e financeira do Poder Judiciário (art. 103-B, §4º, da Constituição Federal) pode coordenar essas centrais de perícia, como forma de viabilizar a padronização e integração. As centrais de perícia devem ser compostas por profissionais qualificados, integrantes dos quadros do Poder Judiciário, uma vez que a garantia da higidez do conteúdo da prova digital é essencial para a realização da própria atividade judicante.

Com a integração entre as centrais de perícia ou com a criação de um núcleo central, seria possível o desenvolvimento e compartilhamento de métodos para a detecção das manipulações a provas digitais.

Essa proposta assemelha-se à estrutura criada em 2004, consistente na Rede Nacional de Genética Forense (RENAGENF) ligada à Secretaria Nacional de Segurança Pública (SENASP). Como bem apontado por Giovanelli e Garrido (2011), essa rede já contava em 2005 com laboratórios em vários estados associados a

vinte e duas universidades do Brasil e serviu como incentivo para a padronização de técnicas e replicação do conhecimento.

O maior obstáculo para a implantação dessa proposta é de ordem orçamentária, uma vez que o Brasil enfrenta grave crise econômica desde 2014. Houve um decréscimo de seu Produto interno bruto na ordem de 5,9% até 2020 (IBGE, 2021), impactando diretamente nos serviços públicos prestados, o que inclui os do Poder Judiciário. Em razão disso, foi promulgada a Emenda Constitucional nº 95 que estabeleceu novo regime fiscal, que limitou o crescimento das despesas públicas por 20 anos. Não se pode deixar de mencionar que a crise econômica foi aprofundada pela pandemia de Sars-Cov-2 ou COVID-19.

Essa limitação orçamentária pode trazer prejuízo à estruturação dessas centrais de perícia, uma vez que além do corpo de profissionais qualificados, também é necessário o investimento em tecnologia e essa seria a segunda proposta para tentar minimizar os impactos negativos da *deepfake* no processo penal.

Sugere-se, ainda, a aquisição ou desenvolvimento pelo Poder Judiciário de *softwares* que permitam o controle da integridade e veracidade da prova digital. A detecção de *deepfake* deve ser feita por meio da utilização de modelos de inteligência artificial baseados em redes neurais especializadas em detecção desse tipo de manipulação (PASHINE et al., 2021).

Existem realmente várias dificuldades para implantação destas soluções sugeridas. Dentre elas, deve ser considerado o alto custo para o desenvolvimento e operação de *softwares* de alto desempenho. A alta tecnologia requer capital intelectual e tecnológico de ponta e a mobilização destes recursos demanda grandes custos. Ainda, devem ser relacionados o baixo desenvolvimento tecnológico do CNJ e dos tribunais brasileiros e a insuficiência do capital intelectual para o desenvolvimento desse tipo de modelo de inteligência artificial.

As questões relativas à propriedade intelectual também precisam ser consideradas, pois os modelos de produção de *deepfake* são *softwares* proprietários e com grande capital intelectual e econômico envolvidos, o que dificulta tanto o desenvolvimento de um novo *software* baseado nos algoritmos dos modelos que produzem *deepfake*, quanto a aquisição dos direitos para uso. Além do mais, os modelos que produzem *deepakes* costumam ser verdadeiras *black-box* (caixa preta), com pouca ou nenhuma transparência. Mesmo os desenvolvedores do modelo costumam ter dificuldades para compreender a resposta produzida, o que impede a explicabilidade e a interpretabilidade das respostas geradas por modelos construídos por abordagens de aprendizado profundo de máquina e redes neurais.

Outra questão relevante para o desenvolvimento de modelo proprietário pelo CNJ e tribunais é a falta de estruturação dos dados. Um dos maiores empecilhos

para o desenvolvimento da inteligência artificial no Brasil é justamente a pouca qualidade das bases de dados, o que os tornam insuficientes para alimentar os algoritmos que dependem de uma extensa e sólida base de dados para o aprendizado e para a categorização desses dados.

Além de todos estes desafios a serem superados, deve-se considerar que os algoritmos que produzem *deepfake* costumam, como dito anteriormente, operar por uma abordagem de inteligência artificial do tipo GANs (redes adversárias generativas), ou seja, é possível que o *deepfake* somente seja reconhecido como tal pelo algoritmo discriminador do algoritmo gerador da falsidade. Ou seja, retorna-se ao problema do *software* proprietário, já que seria exigido do CNJ ou dos tribunais o uso do modelo gerador da *deepfake*.

A terceira proposta está diretamente ligada à tradição existente no Poder Judiciário em que o juiz condutor do processo nomeia um perito de sua confiança para a realização da perícia técnica necessária a conferir o respaldo científico ao elemento de prova.

Neste caso, em termos institucionais, mesmo que alheios à sua estrutura administrativa, deve o Poder Judiciário fomentar a capacitação dos profissionais que atuam nessa área específica. Giovanelli e Garrido (2011) destacam que para a realização de pesquisa na área forense, há a necessidade de ser criada uma comunidade científica, com o escopo de exercer controle sobre a qualidade da produção, bem como haja uma adequada padronização dos métodos e aplicação tecnológica, bem como conceitual.

4 CONSIDERAÇÕES FINAIS

A pesquisa procurou abordar de forma não exaustiva, porém, com suficiente dogmatismo, pontos relevantes pertinentes à inserção de *deepfakes* no processo criminal e à transformação de conteúdos já inseridos no processo em *deepfakes*.

O que se buscou foi analisar as potenciais ameaças geradas, identificando-se alguns riscos à integridade da Justiça Criminal e do Poder Judiciário, assim como à ruptura de princípios fundamentais à ordem democrática.

Como propostas, foi sugerido que sejam criadas centrais de perícia pelos tribunais brasileiros e que os órgãos do Poder Judiciário adquiram ou desenvolvam modelos de inteligência artificial para realizar o controle da integridade e veracidade dos vídeos acostados aos processos criminais. Ainda, sugeriu-se que o Poder Judiciário fomente a capacitação de profissionais de computação forense para que sejam nomeados pelos juízes para a realização de perícia técnica.

Todavia, reconhece-se as dificuldades para a implementação destas

soluções, seja pela insuficiência do capital intelectual e tecnológico do Poder Judiciário brasileiro, seja pelo alto custo financeiro necessário para a aquisição ou desenvolvimento de modelos preditivos, seja por razões de propriedade intelectual, ou, até mesmo, pela falta de estruturação dos dados para o desenvolvimento dos modelos.

O que se conclui é que a questão do uso de *deepfakes* no processo criminal é uma ameaça já presente, é grave, passará a ser usada em processos judiciais e o Poder Judiciário necessita se antecipar e passar a combater os riscos de danos de forma resolutiva. Todavia, trata-se de questão de difícil resolução, ante o permanente progresso das ciências computacionais, que tendem a desenvolver modelos de inteligência artificial cada vez menos transparentes e mais complexos.

Portanto, o estudo sobre o problema proposto não pode ser encerrado por este modesto ensaio. Como mecanismo de antecipação, necessita ser apurado com maior acurácia, para que mais riscos e ameaças possam ser identificados, além da propositura de outras soluções que possam se apresentar mais viáveis do que as propostas neste ensaio.

REFERÊNCIAS

BECK, Ulrich. **Sociedade de risco**: rumo a uma outra modernidade. Tradução Sebastião Nascimento. 2 ed. São Paulo: Editora 34, 2011. 384 p.

CABRAL, Antonio do Passo. Nulidades no processo penal entre garantismo, instrumentalidade e boa-fé: a validade 'prima facie' dos atos processuais. *In*: CALABRICH, Bruno (Org.); FISCHER, Douglas (Org.); PELELLA, Eduardo (Org.). **Garantismo Penal Integral**: questões penais e processuais, criminalidade moderna e a aplicação do modelo garantista no Brasil. 2 ed. Salvador: Juspodivm, 2010, p. 379-410.

CONSELHO NACIONAL DE JUSTIÇA (CNJ). **Justiça em números 2021**. Brasília: CNJ, 2020. 340 p. Disponível em: <https://www.cnj.jus.br/wp-content/uploads/2021/09/relatorio-justica-em-numeros2021-12.pdf>. Acesso em: 30 dez. 2021.

FARID, Hany. An Overview of Perceptual Hashing. **Journal of Online Trust and Safety**, Stanford, v. 1, n. 1. 22 p, 28 out. 2021. Disponível em: <https://doi.org/10.54501/jots.v1i1.24>. Acesso em: 6 jan. 2022.

GICO JR., Ivo Teixeira. A tragédia do Judiciário. **Revista de Direito Administrativo**, v. 267, p. 163-198, 01 set. 2014. Disponível em: <https://doi.org/10.12660/rda.v267.2014.46462>. Acesso em: 3 jan. 2022.

GIOVANELLI, Alexandre; GARRIDO, Rodrigo Grazinoli. A perícia criminal no Brasil como instância legitimadora de práticas policiais inquisitoriais. **Revista Levs**

(**Revista do Laboratório de Estudos da Violência e Segurança da UNESP/Marília**), Marília, v. 7, p. 5-24, 14 dez. 2011. Faculdade de Filosofia e Ciências (UNESP). Disponível em: <https://doi.org/10.36311/1983-2192.2011.v7n7.1672>. Acesso em: 9 jan. 2022.

HALL, Holly Kathleen. Deepfake Videos: When Seeing Isn't Believing. **The Catholic University Journal of Law & Technology**, v. 27, n. 1, p. 51-76, 2018. Disponível em: <https://scholarship.law.edu/jlt/vol27/iss1/4/>. Acesso em: 3 jan. 2022.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA (IBGE). **SCNT - Sistema de Contas Nacionais Trimestrais**. Rio de Janeiro. Disponível em: https://www.ibge.gov.br/estatisticas/economicas/contas-nacionais/9300-contas-nacionais-trimestrais.html?=&t=series-historicas&utm_source=landing&utm_medium=explica&utm_campaign=pib#evolucao-taxa. Acesso em: 10 jan. 2022.

LEVY, Pierre. **O que é o virtual ?**. Tradução Paulo Neves. 2 ed. São Paulo: Editora 34, 2011. 160 p. (Coleção Trans). Tradução de: Qu'est-ce que le virtuel?.

MALLMANN, Felipe Hilgert. **O Processo (Penal) eletrônico e o acesso à justiça no Brasil**. Canoas, 2016. 126 p Dissertação (Programa de Pós-Graduação em Direito e Sociedade) - Centro Universitário La Salle - Unilasalle, Canoas, 2016. Disponível em: <https://svr-net20.unilasalle.edu.br/bitstream/11690/834/1/fhmallmann.pdf>. Acesso em: 22 dez. 2021.

MARAS, Marie-Helen; ALEXANDROU, Alex. Determining authenticity of video evidence in the age of artificial intelligence and in the wake of Deepfake videos. **The International Journal of Evidence & Proof**, New York, v. 23, n. 3, p. 255-262, 01 jul. 2019. doi: 10.1177/1365712718807226. Disponível em: <https://journals.sagepub.com/doi/abs/10.1177/1365712718807226?journalCode=epja>. Acesso em: 5 jan. 2022.

NUCCI, Guilherme de Souza. **Manual de processo penal e execução penal**. 3 ed. São Paulo: Revistas dos Tribunais, 2007. 1022 p.

O'NEILL, Patrick Howell. **The world's top deepfake artist: 'Wow, this is developing more rapidly than I thought.'**: Hao Li sees deepfake technology as moving quickly toward being indistinguishable from reality. MIT Technology Review. Cambridge, 2019. Disponível em: <https://www.technologyreview.com/2019/09/18/132961/the-worlds-top-deepfake-artist-wow-this-is-developing-more-rapidly-than-i-thought/>. Acesso em: 5 jan. 2022.

OLIVEIRA, Eugênio Pacelli de. **Curso de Processo Penal**. 5 ed. Belo Horizonte: Del Rey, 2005. 742 p.

PASHINE, Samay *et al.* Deep Fake Detection: Survey of Facial Manipulation Detection Solutions. **International Research Journal of Engineering and Technology (IRJET)**, Tamilnadu, v. 8, n. 5, p. 4441-4449, mai. 2021. Disponível em: <https://www.irjet.net/archives/V8/i5/IRJET-V8I5811.pdf>. Acesso em: 2 jan. 2022.

PEDRINA, Gustavo Mascarenhas Lacerda. Consequências e perspectivas da aplicação de inteligência artificial a casos penais. **Revista Brasileira de Direito Processual Penal**, Porto Alegre, v. 5, n. 3. 1589–1606 p, 31 out. 2019. Disponível em: <https://doi.org/10.22197/rbdpp.v5i3.265>. Acesso em: 7 jan. 2022.

PFEFFERKORN, Riana. “Deepfakes” in the Courtroom. **Public Interest Law Journal**, Boston, v. 29, n. 2, p. 245-276, 13 set. 2020. Disponível em: <https://www.bu.edu/pilj/archives/vol-29-2-summer-2020/>. Acesso em: 4 jan. 2022.

POLÍCIA FEDERAL. **Operação Lava-Jato**: números. Polícia Federal. Ministério da Justiça e Segurança Pública. Brasília, 2021. Disponível em: <http://www.pf.gov.br/imprensa/lava-jato/numeros-da-operacao-lava-jato>. Acesso em: 2 jan. 2021.

THAMAY, Rennan; TAMER, Maurício. **Provas no direito digital**: conceito da prova digital, procedimentos e provas digitais em espécie. 1 ed. São Paulo: Thomson Reuters Brasil, 2020. 250 p.

TÁVORA, Nestor; ALENCAR, Rosmar Rodrigues. **Curso de Direito Processual Penal**. 11 ed. Salvador: Juspodivm, 2016. 1830 p.

UNIVERSITY OF CALIFORNIA, BERKELEY. **New App Impresses Deepfake Experts Hao Li and Hany Farid**. School of Information. Berkeley, 2019. Disponível em: <https://www.ischool.berkeley.edu/news/2019/new-app-impresses-deepfake-experts-hao-li-and-hany-farid>. Acesso em: 5 jan. 2022.

VAZ, Denise Provasi. **Provas digitais no processo penal**: formulação do conceito, definição das características e sistematização do procedimento probatório. São Paulo, 2012. 198 p Tese (Doutorado em Direito Processual) - Universidade de São Paulo (usp), São Paulo, 2012. Disponível em: <https://teses.usp.br/teses/disponiveis/2/2137/tde-28052013-153123/pt-br.php>. Acesso em: 5 jan. 2022.

VIDAL, Sávaia Cristina; SANTOS, Kayque Luiz Farias dos; NOGUEIRA, Ronaldo. Sistemas de Numeração com Ênfase no Sistema Binário e sua Aplicação por meio da Álgebra de Boole. **Jornada Científica**, Lorena, v. 1, n. 2. 17 p, 11 fev. 2016. Disponível em: <http://www.revista.unisal.br/lo/index.php/revistajornada/article/view/491>. Acesso em: 5 jan. 2022.

WESTERLUND, Mika. The Emergence of Deepfake Technology: A Review. **Technology Innovation Management Review**, Ottawa, v. 9, n. 11, p. 39-52, nov. 2019. Disponível em: <https://timreview.ca/article/1282>. Acesso em: 3 jan. 2022.

WIGGERS, Kyle. **Generative adversarial networks**: What GANs are and how they’ve evolved. VentureBeat. San Francisco, 2019. Disponível em: <https://venturebeat.com/2019/12/26/gan-generative-adversarial-network-explainer-ai-machine-learning/>. Acesso em: 2 jan. 2022.

XIAO, Weibing. A situação jurídica da China na área do acesso à informação. **Revista CEJ**. Tradução Ricardo Perlingeiro, Brasília, v. 19, n. 66, p. 7-16, mai./ago.

2015. Tradução de: The legal situation in China regarding information access.
Disponível em: <https://revistacej.cjf.jus.br/cej/index.php/revcej/article/view/2037>.
Acesso em: 9 jan. 2022.