

XXX CONGRESSO NACIONAL DO CONPEDI FORTALEZA - CE

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS I

CARLOS MARDEN CABRAL COUTINHO

JOSÉ RENATO GAZIERO CELLA

YURI NATHAN DA COSTA LANNES

Todos os direitos reservados e protegidos. Nenhuma parte destes anais poderá ser reproduzida ou transmitida sejam quais forem os meios empregados sem prévia autorização dos editores.

Diretoria - CONPEDI

Presidente - Profa. Dra. Samyra Haydêe Dal Farra Naspolini - FMU - São Paulo

Diretor Executivo - Prof. Dr. Orides Mezzaroba - UFSC - Santa Catarina

Vice-presidente Norte - Prof. Dr. Jean Carlos Dias - Cesupa - Pará

Vice-presidente Centro-Oeste - Prof. Dr. José Querino Tavares Neto - UFG - Goiás

Vice-presidente Sul - Prof. Dr. Leonel Severo Rocha - Unisinos - Rio Grande do Sul

Vice-presidente Sudeste - Profa. Dra. Rosângela Lunardelli Cavallazzi - UFRJ/PUCRio - Rio de Janeiro

Vice-presidente Nordeste - Prof. Dr. Raymundo Juliano Feitosa - UNICAP - Pernambuco

Representante Discente: Prof. Dr. Abner da Silva Jaques - UPM/UNIGRAN - Mato Grosso do Sul

Conselho Fiscal:

Prof. Dr. José Filomeno de Moraes Filho - UFMA - Maranhão

Prof. Dr. Caio Augusto Souza Lara - SKEMA/ESDHC/UFMG - Minas Gerais

Prof. Dr. Valter Moura do Carmo - UFERSA - Rio Grande do Norte

Prof. Dr. Fernando Passos - UNIARA - São Paulo

Prof. Dr. Edinilson Donisete Machado - UNIVEM/UENP - São Paulo

Secretarias

Relações Institucionais:

Prof. Dra. Claudia Maria Barbosa - PUCPR - Paraná

Prof. Dr. Heron José de Santana Gordilho - UFBA - Bahia

Profa. Dra. Daniela Marques de Moraes - UNB - Distrito Federal

Comunicação:

Prof. Dr. Robison Tramontina - UNOESC - Santa Catarina

Prof. Dr. Liton Lanes Pilau Sobrinho - UPF/Univali - Rio Grande do Sul

Prof. Dr. Lucas Gonçalves da Silva - UFS - Sergipe

Relações Internacionais para o Continente Americano:

Prof. Dr. Jerônimo Siqueira Tybusch - UFSM - Rio Grande do sul

Prof. Dr. Paulo Roberto Barbosa Ramos - UFMA - Maranhão

Prof. Dr. Felipe Chiarello de Souza Pinto - UPM - São Paulo

Relações Internacionais para os demais Continentes:

Profa. Dra. Gina Vidal Marcilio Pompeu - UNIFOR - Ceará

Profa. Dra. Sandra Regina Martini - UNIRITTER / UFRGS - Rio Grande do Sul

Profa. Dra. Maria Claudia da Silva Antunes de Souza - UNIVALI - Santa Catarina

Eventos:

Prof. Dr. Yuri Nathan da Costa Lannes - FDF - São Paulo

Profa. Dra. Norma Sueli Padilha - UFSC - Santa Catarina

Prof. Dr. Juraci Mourão Lopes Filho - UNICHRISTUS - Ceará

Membro Nato - Presidência anterior Prof. Dr. Raymundo Juliano Feitosa - UNICAP - Pernambuco

D597

Direito, Governança e novas tecnologias I [Recurso eletrônico on-line] Organização CONPEDI

Coordenadores: Carlos Marden Cabral Coutinho; José Renato Gaziero Cella; Yuri Nathan da Costa Lannes. – Florianópolis: CONPEDI, 2023.

Inclui bibliografia

ISBN: 978-65-5648-813-4

Modo de acesso: www.conpedi.org.br em publicações

Tema: Saúde: Acesso à justiça, Solução de litígios e Desenvolvimento

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Direito. 3. Governança e novas tecnologias. XXX Congresso Nacional do CONPEDI Fortaleza - Ceará (3; 2023; Florianópolis, Brasil).

CDU: 34



XXX CONGRESSO NACIONAL DO CONPEDI FORTALEZA - CE

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS I

Apresentação

No XXX Congresso Nacional do CONPEDI, realizado nos dias 15, 16 e 17 de novembro de 2023, o Grupo de Trabalho - GT “Direito, Governança e Novas Tecnologias I”, que teve lugar na tarde de 15 de novembro de 2023, destacou-se no evento não apenas pela qualidade dos trabalhos apresentados, mas pelos autores dos artigos, que são professores pesquisadores acompanhados de seus alunos pós-graduandos. Foram apresentados 23 (vinte e três) artigos objeto de um intenso debate presidido pelos coordenadores e acompanhado pela participação instigante do público presente na Faculdade de Direito do Centro Universitário Christus - UNICHRISTUS.

Esse fato demonstra a inquietude que os temas debatidos despertam na seara jurídica. Cientes desse fato, os programas de pós-graduação em direito empreendem um diálogo que suscita a interdisciplinaridade na pesquisa e se propõe a enfrentar os desafios que as novas tecnologias impõem ao direito. Para apresentar e discutir os trabalhos produzidos sob essa perspectiva, os coordenadores do grupo de trabalho dividiram os artigos em cinco blocos, quais sejam a) temas de inteligência artificial; b) temas de liberdade de expressão e fake news; c) temas de proteção de dados pessoais; d) temas de cidadania, democracia, constituição e direitos; e e) temas de regulação.

Os artigos que ora são apresentados ao público têm a finalidade de fomentar a pesquisa e fortalecer o diálogo interdisciplinar em torno do tema “Direito, Governança e Novas Tecnologias”. Trazem consigo, ainda, a expectativa de contribuir para os avanços do estudo desse tema no âmbito da pós-graduação em direito, apresentando respostas para uma realidade que se mostra em constante transformação.

Os Coordenadores

Prof. Dr. Carlos Marden Cabral Coutinho - Centro Universitário Christus

Prof. Dr. José Renato Gaziero Cella - Atitus Educação

Prof. Dr. Yuri Nathan da Costa Lannes - Faculdade de Direito de Franca

**PROVA DIGITAL AUTOMATIZADA NO SISTEMA PROCESSUAL BRASILEIRO:
CONFORMIDADE ÉTICO-NORMATIVA DA PRODUÇÃO PROBATÓRIA**

**AUTOMATED DIGITAL EVIDENCE IN BRAZILIAN PROCEDURAL SYSTEM:
THE EVIDENCE PRODUCTION ETHICAL AND NORMATIVE CONFORMITY**

**Isabelle Brito Bezerra Mendes
Luis Henrique De Menezes Acioly
João Araújo Monteiro Neto**

Resumo

A inserção da administração da justiça e do processo judicial no âmbito digital tem trazidos desafios de grande envergadura, especialmente quanto em voga a compatibilização de direitos fundamentais dos jurisdicionados com a eficiência e celeridade da justiça. No âmbito processual, a prova digital tem ganhado relevância, na medida em que concerne a uma relevante discussão sobre legitimidade e validade jurídicas. A inserção de ferramentas de inteligência artificial acresce o debate, com considerações sobre ética e conformidade. Busca o presente estudo traçar um delineamento de parâmetros ético-normativos para o uso de inteligência artificial na produção da prova digital, tendo em vista sopesar a sua legitimidade e proteção de direitos fundamentais, com a acurácia, no contexto social de digitalização da vida. Empreendeu-se, para tanto, uma revisão literária por meio de uma pesquisa bibliográfica, de cunho descritivo e natureza qualitativa. Obteve-se como resultado que a produção de provas digitais automatizadas deve ser pautada por um conjunto ético-normativo, essencialmente relacionados à privacidade, explicabilidade e mitigação de vieses discriminatórios, que sejam coerentes com o estado da arte sobre ética no uso e desenvolvimento de IA, a partir de influxos de coordenação com as normas esparsas aplicáveis às provas digitais. Observou-se, ainda, que a aplicação de diretrizes de conformidade ético-normativa se coaduna com contexto da transformação do Poder Judiciário brasileiro, no âmbito da Justiça 4.0 e incorporação de sistemas de inteligência artificial.

Palavras-chave: Provas digitais, Inteligência artificial, Processo penal, Justiça 4.0, Ética

Abstract/Resumen/Résumé

The insertion of the administration of justice and the judicial process in the digital sphere has brought major challenges, especially when it comes to making the fundamental rights of those under jurisdiction compatible with the efficiency and speed of justice. In the procedural sphere, digital evidence has gained relevance, as it concerns a relevant discussion about legal legitimacy and validity. The insertion of artificial intelligence tools adds to the debate, with considerations about ethics and compliance. This study seeks to outline an outline of ethical-normative parameters for the use of artificial intelligence in the production of digital

evidence, with a view to weighing its legitimacy and protection of fundamental rights, with accuracy, in the social context of digitalization of life. To this end, a literary review was undertaken through bibliographical research, of a descriptive nature and qualitative nature. The result was that the production of automated digital evidence must be guided by an ethical-normative set, essentially related to privacy, explainability and mitigation of discriminatory biases, which are coherent with the state of the art on ethics in the use and development of AI , based on coordination inputs with the sparse standards applicable to digital evidence. It was also observed that the application of ethical-normative compliance guidelines is in line with the context of the transformation of the Brazilian Judiciary, within the scope of Justice 4.0 and the incorporation of artificial intelligence systems.

Keywords/Palabras-claves/Mots-clés: Digital evidence, Artificial intelligence, Criminal proceedings, 4.0 justice, Ethics

1 INTRODUÇÃO

A transformação digital tem apresentado grandes influxos na sociedade, e por conseguinte à administração do sistema de justiça nacional e ao processo judicial em si. O uso paulatino de novas tecnologias tem representado um grande avanço a título de celeridade, eficiência e garantia do direito de acesso, na mesma medida em que as normas sobre o tema ganham a necessidade de atualização constante. Como marcos no Poder Judiciário brasileiro, o movimento da Justiça 4.0, como fomento à inovação, e a Resolução n. 332, de 2020, do Conselho Nacional de Justiça, em que se regulamentou parâmetros para a governança do uso de Inteligência Artificial nos tribunais, representaram a nova face da justiça brasileira.

Não somente em relação à estrutura destinada à administração da justiça que se apontam influxos das tecnologias, mas a própria questão processual tem sido afetada pela realidade intrinsecamente ligada às ferramentas digitais. No âmbito processual, muito tem se discutido sobre a admissibilidade das provas digitais, especialmente quanto ao Processo Penal, em que vigoram regras específicas sobre a produção de prova, tendo em vista a predominância do rigor legislativo de prescrição normativa. Esse panorama se acresce à inserção de sistemas de inteligência artificial, com relevantes discussões sobre ética, combate à discriminação algorítmica e eficiência e acurácia, circunstância ora denominada de Prova Digital Automatizada. Descortina-se, assim, um horizonte de dúvidas sobre a legitimidade do uso de mecanismos de inteligência artificial no inserto contexto das provas digitais em âmbito processual penal.

Ante essa celeuma jurídico-social, o presente artigo se ergue na busca de traçar um delineamento de parâmetros ético-normativos para o uso de inteligência artificial na produção da prova digital, tendo em vista sopesar a sua legitimidade e proteção de direitos fundamentais, com a acurácia, no contexto social de digitalização da vida. Tem-se por objetivo também, compreender a conceituação e características da prova digital, bem como entender o seu *locus* topográfico na teoria geral da prova. Tem-se por objetivo também entender e evidenciar as nuances que envolvem a aplicabilidade de mecanismos de inteligência artificial no contexto probatório. Ademais, busca-se consignar o atual panorama da discussão sobre a ética no uso e desenvolvimento de inteligência artificial.

Para tanto, optou-se por realizar uma revisão literária por meio de uma pesquisa bibliográfica – de cunho descritivo e natureza qualitativa –, cuja coleta de dados se deu por livros, dissertações e artigos em bases de dados eletrônicas, tendo como descritores: processo penal; inteligência artificial; prova digital; ética em IA; Justiça 4.0. A metodologia empreendida na presente pesquisa pretendeu preconizar a compatibilização e diálogo entre a doutrina clássica

com manuscritos recentes, através da metodologia jurídico-compreensiva, proposta por Gustin, Dias e Nicácio (2020).

O presente artigo tem o seu desenvolvimento subdividido em cinco capítulos e a conclusão. O primeiro capítulo diz respeito à contextualização sobre a inovação judicial no âmbito da administração da justiça brasileira e no processo judicial. O segundo capítulo aponta delineamentos gerais sobre a teoria geral da prova, ao passo que o terceiro capítulo conceitua e consigna a aplicabilidade da prova digital. O quarto capítulo aponta os resultados quanto ao conceito e ao contexto da prova digital automatizada. O quinto capítulo apresenta as questões envolvendo a admissibilidade normativa e pressupostos éticos que devem nortear a produção da prova digital automatizada. Ao cabo são tecidas as considerações finais.

2 INOVAÇÃO DIGITAL NA JUSTIÇA E NO PROCESSO JUDICIAL BRASILEIRO

A organização jurisdicional de uma comunidade é reflexo direto de suas características culturais, econômicas e políticas. Dessa forma, o despontamento de novas formas de tecnologia da informação aponta direta e frontalmente para consequências no direito e na justiça (ARAÚJO; GABRIEL, 2022), o que representa um ponto de atenção ao processo penal já que inevitavelmente haverá uma pressão para que as normas sejam capazes de abarcar a realidade imposta.

Nesse contexto, Schwab (2019, p. 20) explica que na virada do século deu-se o início da quarta revolução industrial e está baseada numa revolução digital, sendo caracterizada “por uma internet mais ubíqua e móvel, por sensores menores e mais poderosos que se tornaram mais baratos e pela inteligência artificial e aprendizagem automática (ou aprendizado de máquina)”. Nesse mesmo sentido, Madalena (2021) e Jenkins (2009) apontam que a revolução contemporânea na comunicação decorre do processo de transformação de uma sociedade analógica para um modelo organizacional pautado na *hyper-informação*.

Entretanto, a diferença dessa revolução para as outras é que ela toca simultaneamente todas as áreas do conhecimento, resultando na interação constante dos domínios físicos, digitais e biológicos, e, por essa razão, as tecnologias e as inovações são difundidas de uma forma muito mais rápida e ampla. Assim, Schwab (2019), apesar de entender a importância e o tamanho do impacto, aponta que há alguns pontos que o preocupam e que “que podem limitar a realização efetiva e coesa da quarta revolução industrial” (SCHWAB, 2019, p. 21).

Schwab (2019), Lee (2019) e Jenkins (2009) trazem à tona um problema que já é evidente na sociedade atual e tem causado uma série de dificuldades para que o uso da

tecnologia seja efetivo e a inovação alcance o desenvolvimento que se pretende. Esse problema concerne à falta de alinhamento entre a realidade avançada do desenvolvimento tecnológico, em contraste com a pouca compreensão e domínio das consequências advindas dessa realidade, bem como à entrega de soluções adequadas às lacunas geradas.

Quando se trata de tecnologias e inovação, as normativas devem ser as mais atuais possíveis, visto que as mudanças, muitas vezes de um ano para outro, são substanciais. O problema da ausência de ritmo do direito em acompanhar a sociedade (KELLER, 2019) alcança estruturas analógica e digitais, conduzindo a questões específicas ao acesso eficaz à justiça (TAUK; SALOMÃO, 2023). Quanto ao direito penal e processo penal, esse contexto de descolamento do direito da realidade não se adstringe à morosidade e burocracia dos processos legislativos (JESUS; MILAGRE, 2016), mas também e principalmente à falta de interesse do legislador em viabilizar a adequação do ordenamento à realidade interconectada (CASTELLS, 2002).

No contexto do acesso à justiça, a transformação digital do poder judiciário tem conduzido a um panorama de paulatina inserção de mecanismos tecnológicos no cerne do funcionamento das estruturas da justiça (ARAÚJO; GABRIEL, PORTO, 2022). À guisa de exemplo, o Tauk e Salomão (2023) apontam que foi identificado 64 (sessenta e quatro) ferramentas de Inteligência Artificial no Poder Judiciário brasileiro, espalhados por 44 (quarenta e quatro) tribunais. As medidas concernentes à transformação digital do Poder Judiciário, em grande parte se devem ao programa chamado *Justiça 4.0*, pelo Conselho Nacional de Justiça, iniciado em janeiro de 2021 com apoio do Programa das Nações Unidas para o Desenvolvimento (RAMPIM; IGREJA, 2022). Estão inseridos nesse programa iniciativas como a “Plataforma Digital do Poder Judiciário, a Plataforma Sinapses/Inteligência Artificial, a Plataforma Codex, o Balcão Virtual, os Núcleos de Justiça 4.0 e o Juízo 100% Digital” (RAMPIM; IGREJA, 2022, p. 125).

Trazendo essa realidade para a reflexão a que se propõe esse estudo, busca-se refletir sobre a necessidade de uma resposta do processo penal no que diz respeito às provas digitais. Vale lembrar que processo penal, especificamente, também é reflexo direto da sociedade na qual está inserido (VAZ, 2012) e além de incorporar em sua dinâmica as ferramentas tecnológicas, também precisa apresentar soluções coerentes às lacunas que se apresentam. O deslocamento das relações digitais para o palco virtual (LÉVY, 1996) não tem revelado apenas bons frutos (ACIOLY, 2021), mas tem viabilizado também novas formas de cometimentos de crimes, no âmbito das interconexões digitais, cuja amplitude e velocidade de resposta ainda se mostram lentos (JESUS; MILAGRE, 2016).

Especificamente no que diz respeito às provas, os estudos do impacto dessa evolução tecnológica no processo penal ainda são muito incipientes (MINTO, 2021). Apesar de atualmente muito se utilizar a prova digital como fundamento de investigações e acusações, não estão completamente definidos todos os processos de admissibilidade, quais são as autorizações legais de obtenção dessas provas, e nem mesmo há uma compreensão fechada sobre o que realmente se configura prova digital. Ou seja, a prova digital tem sido usada na prática penal cotidiana, mas não está totalmente regulamentada.

3 DELINEAMENTOS GERAIS SOBRE A TEORIA GERAL DA PROVA

Antes de se passar para o estudo da prova digital propriamente dito, há que se abordar pontos essenciais da Teoria Geral da Prova, para que se chegue então ao efetivo conhecimento e entendimento do que se trata a prova digital. Existem dois modelos de processo, o inquisitório e o acusatório, a depender do modelo os papéis dos sujeitos e as oportunidades de atuação conferidas podem diferir (TÁVORA; ALENCAR, 2022). Sem embargo da discussão quanto à estruturação sistêmica dos postulados que concernem aos modelos processuais penais (LOPES JÚNIOR, 2021), filia-se, no presente estudo, à compreensão de Távora e Alencar (2022) e de Capez (2023), para quem o Brasil adota o modelo acusatório, pautado nos axiomas da Constituição Federal de 1988, o presente trabalho irá ater-se às características e ponderações referentes a ele.

No ideal do modelo acusatório preza-se pela busca da verdade formal, baseando-se na estrita legalidade e na importância da produção probatória para condução do devido processo legal, permitindo-se o contraditório e a ampla defesa (CAPEZ, 2023; PACELLI, 2023; TÁVORA; ALENCAR, 2022). Segundo o artigo 155 do Código de Processo Penal - Decreto-Lei nº 3.689/1941, ou CPP -, o juiz deve formar sua convicção mediante a livre apreciação das provas produzidas em contraditório judicial. Há, portanto, “a aplicação do sistema do livre convencimento, em que os juízes, não atrelados a regras rígidas acerca do valor das provas, valoram-nas conforme sua convicção, de maneira motivada (VAZ, 2012, p. 38). Lopes Junior (2021, p. 153) ressalta, ainda, que “processo penal e a prova nele admitida integram o que se poderia chamar de modos de construção do convencimento do julgador”.

Vale pontuar que o sistema processual brasileiro está ancorado no conceito de devido processo legal, conforme depreende-se da dicção do artigo 5º, inciso LIV, da Constituição Federal de 1988, e que aponta diretamente para sua configuração garantista (CAPEZ, 2023; TÁVORA; ALENCAR, 2022). Dessa forma, o processo deve não apenas representar o efetivo

exercício da jurisdição, mas também a segurança aos indivíduos de que seus direitos serão preservados.

Levando em consideração sua relevância, o direito a prova é reconhecido como uma das garantias do devido processo legal, “podendo-se vislumbrá-lo na garantia da plenitude de defesa” (VAZ, 2012, p. 41) e que engloba todos os processos necessários para que o indivíduo atinja seu objetivo. Apesar disso, vale ressaltar que não se trata de um direito absoluto e que também é submetido a limitações, um conjunto de regras que direcionam o método probatório judiciário (VAZ, 2012).

Sendo assim, a prova é o meio pelo qual é formada a convicção do juiz em relação a um fato específico (THAMAY; TAMER, 2022), desde que estejam de acordo com a forma da lei, sendo também levado em consideração a relevância da prova para o caso, seu meio de obtenção e sua produção. Mediante essa conceituação é possível observar que o vocábulo prova pode ser utilizado em três aspectos diferentes, que são as fontes de provas, os meios de prova e os elementos de prova.

Fonte de prova é tudo que for apto para permitir a produção de uma prova, como uma pessoa, um cadáver ou um escrito, por exemplo (MINTO, 2021). Meio de prova, já se refere ao instrumento pelo qual uma prova é introduzida no processo, refere-se a forma que a fonte de prova foi levada ao juiz para seu conhecimento (MINTO, 2021). Finalmente, elemento de prova é exatamente o dado que confirma ou nega uma asserção a respeito do fato que interessa à decisão da causa (MINTO, 2021). Assim, a prova refere-se aos instrumentos aptos à produção, a explicação e comprovação.

Ademais, a prova, portanto, deve ter estrita ligação com o fato, deve ser obtida dentro dos padrões legais, bem como deve ser advinda de uma fonte válida. Fora disso, segundo o artigo 157 do Código de Processo Penal, as provas são passíveis de inadmissibilidade no contexto processual. Nesse contexto vale introduzir a divisão existente entre provas típicas e atípicas, com o conceito apresentado por Laronga (2002), quando diz que a prova típica é aquela que é prevista e possui procedimento próprio para que seja efetivada, já a prova atípica não possui nenhum tipo de procedimento para sua produção, podendo ser prevista ou não. Nesse sentido Fernandes, Almeida e Moraes (2011) apontam que as caracterizações sobre atipicidade da prova decorrem de situações que circunscrevem ao meio de obtenção ou produção, a consequente normatização de suas características.

É possível compreender, então, que há possibilidades de aceite de uma prova mesmo que ela não esteja prevista ou que não tenha procedimento estabelecido. Lopes Júnior (2011) explica que, pode-se aceitar excepcionalmente provas atípicas, desde que dentro dos limites

constitucionais e processuais. Dessa forma, as provas devem ser viabilizadas de acordo com as configurações com o que o fato a ser provado se apresenta.

A realidade da prova se apresentar como um direito constitucional fundamental impede que seja desconsiderada às partes, principalmente sob o argumento da ausência de um meio típico (THAMAY; TAMER, 2022, p.18), já que são meios e recursos inerentes a garantia do contraditório e da ampla defesa. Com isso, a prova não pode ser rejeitada apenas em razão de sua atipicidade, em se tratando de um direito constitucional e, se lícita para provar os fatos do caso, o direito deve dar suporte à recepção da prova, o que nos aproxima cada vez mais da viabilidade de utilização da prova digital. Cita-se a análise realizada por Thamay e Tamer (2022, p. 19) quanto à admissibilidade dos meios probatórios:

O acesso à função jurisdicional adequada é aquele vocacionado e que se viabiliza pelo mais próximo ou perfeito ajuste entre os instrumentos processuais e os direitos materiais postos. Nesse sentido, considerando que os direitos materiais se perfazem em suportes fáticos e esses são demonstrados a partir dos meios probatórios, nada mais coerente que o ordenamento processual viabilize a realização da prova e que tal atividade goze das possibilidades ajustadas à realidade.

Portanto, se a prova estiver apta a demonstrar a veracidade de um fato e estiver dentro dos parâmetros de legalidade não há por que dispensar a prova. Entretanto, não se pode esquecer que a admissibilidade da prova atípica, diferentemente da típica, deve ser submetida a critérios mais rígidos e deve ser entendida como excepcional.

4 PROVA DIGITAL: CONCEITO E APLICABILIDADE

O conceito de prova digital, assim como o conceito de prova no sentido estrito, não é pacífico, é possível encontrar múltiplos sentidos. Casey (2011, p. 17), em seu livro “*Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*” adota a definição de que prova digital corresponde a “quaisquer dados armazenados ou transmitidos usando um computador que apoiem ou refutem uma teoria de como ocorreu um crime ou que abordem elementos críticos do crime, como intenção ou álibi”.

A *Scientific Working Group on Digital Evidence* (SWGDE) e a *International Organization on Digital Evidence* (IOCE), em um documento que define os Padrões e Princípios da prova digital (*Digital Evidence: Standards and Principles*), traz a seguinte definição: “Informações de valor probatório armazenadas ou transmitidas em formato digital”. Nesse contexto, Minto (2021, p. 15) entende que “o termo prova digital se refere a dados

produzidos e processados a partir da lógica binária – dados digitais – e que têm potencial para serem utilizados como fonte de prova no processo penal”. A seu turno, Thamay e Tamer (2022, p. 32) entendem que prova digital poderá ter duas acepções: uma relacionada à demonstração de um fato ocorrido em meios digitais; e outra, relacionada à demonstração por meio digital da ocorrência de um fato.

Pode-se, nesse âmbito, valer-se da conceituação trazida por Vaz (2012, p. 63), que em sua tese define prova digital como “os dados em forma digital (no sistema binário) constantes de um suporte eletrônico ou transmitidos em rede de comunicação, os quais contêm a representação de fatos ou ideia.” Dessa forma, observa-se que provas digitais são meios de demonstração de uma situação ocorrida dentro do contexto digital, ou cujos dados armazenados digitalmente sejam suficientes para explicar um fato.

Pode-se, ainda, apontar que a peculiaridade da prova digital consiste na forma de arquivamento de informações e suas características, de forma que em cotejo as demais provas do processo, entendessemos que a prova digital caracteriza-se como fonte de prova, sobre a qual pode se extrair evidências relevantes à persecução penal (VAZ, 2012).

Pontua-se que, mediante o que foi acima exposto, a prova digital não se confunde com a prestação de informações feitas por meio eletrônico, que está ali como uma ferramenta facilitadora da coleta de outro tipo de prova, nem mesmo com outros meios de prova que fazem uso de sistemas informáticos para o auxílio na análise e interpretação de dados contidos no processo (VAZ, 2012). Nesse contexto, Lupária (2007) atribui o conceito de *computer-generated-evidence* às animações e simulações feitas com auxílio de sistemas informáticos. Além do que, não deve ser confundida com prova eletrônica, que segundo Casey (2011) seria o gênero que comporta a espécie que é a prova digital, abrangendo, inclusive, o suporte físico que armazena os dados digitais.

No que se refere às suas características, a prova digital tem atributos próprios que merecem ser levados em consideração, principalmente no que diz respeito ao seu registro, extração, conservação e apresentação em juízo, pois são estes que a individualizam como categoria específica de fonte de prova (VAZ, 2012). As características da prova digital, além de atribuírem um vetor de identificação, contribuem para delimitar questões envolvendo a sua recolha, custódia e validade (CASTIGLIONE et al, 2013).

A partir da revisão literária empreendida (VAZ, 2012; MINTO, 2021; CASTIGLIONE et al, 2013), é possível perceber que há entendimento pacífico de pelo menos três características das provas digitais, são elas a imaterialidade, a volatilidade ou fragilidade e dispersão. A imaterialidade é referente a natureza impalpável dos dados que se referem a prova digital (VAZ,

2012) e que existem independentemente de qualquer suporte físico (MINTO, 2021). A volatilidade, ou fragilidade, diz respeito à facilidade de alteração ou desaparecimento a que está submetido, ou seja, não há fixação material da prova (VAZ, 2012; CASTIGLIONE et al, 2013). Assim a prova pode desaparecer em razão de determinados eventos, sendo intencionais ou não (MINTO, 2021). Por fim, o potencial de dispersão da prova refere-se à possibilidade de estar localizada em vários locais diferentes ao mesmo tempo, tanto no sentido geográfico quanto no sentido informático (MINTO, 2021, p. 36).

Atentar para as particularidades da prova digital é fundamental para que se traga a solução devida à realidade que se impõe e não tente apenas imputar recursos antigos, referentes a outro cenário, imaginando ser a ação mais coerente. As especialidades da prova digital aqui apontadas não são abordadas no estudo tradicional das provas, nem por isso devem ser desprezadas ou impedidas de uso, demandando que seus meios de obtenção sejam mais bem regulados e especificados.

5 PROVA DIGITAL AUTOMATIZADA E USO DE INTELIGÊNCIA ARTIFICIAL

Como já exposto anteriormente, o crescimento digital acelerado, as novas tecnologias e o desenvolvimento massivo da Inteligência Artificial têm afetado diretamente o cotidiano social e conseqüentemente o direito. Segundo Lee (2019) e Ford (2021), na última década o campo da Inteligência Artificial deu um salto revolucionário e está a começar a fornecer um número cada vez maior de aplicações práticas que têm inegavelmente transformado o mundo ao nosso redor.

Em razão do grande desenvolvimento computacional, com ferramentas efetivamente capazes de realizar o que anteriormente estava apenas no imaginário dos cientistas, e da grande quantidade de dados gerados e recolhidos, é possível treinar e desenvolver as máquinas para que cheguem aos resultados esperados e tragam automatizações cada vez mais surpreendentes. A Inteligência Artificial, nesse contexto, ainda possui questões desconhecidas, que podem gerar riscos reais não somente aos indivíduos como a uma sociedade completa (FORD, 2021).

Frente a esse panorama se traz à tona o influxo da Inteligência Artificial no que diz respeito as provas digitais. Há que se levar em consideração não apenas a existência de provas digitais, advindas da presença intrínseca da tecnologia no cotidiano social, mas da possibilidade real de se automatizar a produção dessas provas. Com o avanço da ciência de dados e computação forense, novas ferramentas de produção de prova tem se apresentado no cotidiano forense.

Com auxílio de ferramentas de Inteligência Artificial, pautadas em *machine learning*, a ciência forense tem se aplicado em descobrir padrões em dados brutos, identificar evidências ocultas e fornecer informações relevantes (PADILHA et al, 2021). O *machine learning* tem suas aplicações em investigações forenses voltadas ao escopo de descoberta de informações, triagem de dispositivos e investigações em rede (SAXENA et al, 2023), atribuindo sentido aos processos de classificação, agrupamento, ou “*clusters*” e regressão (SILVA FILHO, 2016; CARVALHO et al, 2015).

Quanto à usabilidade de ferramentas de IA na produção de prova digitais, Albino e Lima (2023) sintetizam aplicação em: (i) extração de metadados de documentos digitais; (ii) análise e reconhecimento de voz; (iii) análise de autenticidade de vídeos; (iv) análise de linguagem natural; (v) análise de autenticidade de fotografias digitais; (vi) identificação de padrões de dados; (vii) análise de interações em redes sociais.

O uso de Inteligência Artificial no processo forense tem seguido à dinâmica social de incorporação dessa espécie de ferramenta tecnológica no cotidiano das relações, especialmente nas chamadas redes sociais e interações via internet (PADILHA et al, 2021; CARVALHO et al, 2015; HASSAN, 2019).

A extração e análise metadados ganha especial destaque na medida em que sua aplicabilidade se estende a toda espécie de arquivo digital, fornecendo informações importantes sobre os dados, como formato, autor, localização geográfica do IP e caminho digital e data de criação e modificação (ALBINO; LIMA, 2023; CARVALHO et al, 2015). Padilha et al (2021) apontam que a filtragem de informações é o primeiro processo forense, tendo em vista a quantidade de metadados que acompanham cada documento ou arquivo.

Tomando-se como exemplo, Padilha et al (2021), Albino e Lima (2023) e Silva Filho (2016) apontam que a mera publicação em redes sociais tem o condão de gerar uma gama de informações, compartilhadas e difundidas na internet, para além do uso lícito de dados pessoais. Tais informações podem ser coletadas por meio de APIs fornecidas pelas próprias redes, ou por meio de raspagem de dados (PADILHA et al, 2021), o que demanda específica metodologia de preservação de sua integridade e de garantia de sua cadeia de custódia (SILVA FILHO, 2016; HASSAN, 2019).

A utilização direta da tecnologia, especialmente inteligência artificial, para busca de evidências, de forma célere e autônoma. Vale ressaltar que podem ser utilizadas tanto de forma preventiva, antes da ocorrência de um incidente, ou reativa, após a ocorrência do mesmo (IRONS; LALLIE, 2014). Atualmente essa técnica tem sido utilizada em situações de procura de informações pelos serviços secretos e militares, bem como *law enforcement agencies* no

Reino Unido, na Europa e nos Estados Unidos (IRONS; LALLIE, 2014).

Dos breves exemplos citados é possível perceber que se está diante de uma realidade com possibilidades reais de rápida difusão e uso, mas que ao mesmo tempo não possui normas de direcionamento de seu uso, diretrizes delimitadoras da aplicabilidade da Inteligência Artificial nesse sentido e nem padrões éticos que garantam a coerência da ferramenta e a sua consequente preservação dos direitos e garantias fundamentais. Enfrenta-se agora os desdobramentos da inovação.

Provas digitais requerem um tratamento diferenciado, não podendo se submeter ao método de produção de provas tradicional. Precisam muitas vezes ser obtidas antes que a questão se torne um problema e seja requerido em justiça, precisam ser acessadas em território de terceiros, ou até mesmo precisam ser obtidas por meio de uma intervenção direta nas comunicações. Submetê-las simplesmente ao método tradicional, não apenas prejudicará sua possibilidade de utilização e produção, como também não trará a devida preservação de direitos e garantias fundamentais.

6 ADMISSIBILIDADE ÉTICO-NORMATIVA DAS PROVAS DIGITAIS AUTOMATIZADAS

De uma forma geral, não há no Brasil uma normativa específica no que diz respeito as provas digitais, e nem mesmo relativa à influência de uma inteligência artificial nesse sentido. E, frente ao que foi exposto até o momento, é possível compreender que há uma diferença significativa entre o meio de prova aqui apresentado e os meios de provas típicos, previstos nas normativas atuais. Então há necessidade de um direcionamento normativo específico ao contexto digital, abarcando, inclusive questões éticas envolvendo o manejo de inteligência artificial.

6.1 Conformidade Normativa das Provas Digitais

No que diz respeito ao Brasil, no ano de 2001, foi assinada a Convenção de Budapeste, também conhecida como convenção do cibercrime, que tinha o objetivo de definir de forma harmônica os crimes praticados no meio digital, bem como as formas de persecução. Atualmente é o documento referencial no âmbito internacional nesse contexto e o Brasil tem esse texto incorporado a jurisdição pátria.

Entre várias questões a convenção de Budapeste trata de quatro temas principais: (a) criminalização de condutas; (b) normas para investigação; (c) produção de provas eletrônicas; e (d) meios de cooperação internacional, como extradição e assistência jurídica mútua.

No que se refere especificamente à produção de provas, a Convenção de Budapeste aponta quatro meios principais. O primeiro, que se encontra nos artigos 16 e 17, trata da conservação expedita de dados informáticos armazenados. Seria exatamente a possibilidade que autoridades competentes têm de ordenar a preservação de dados informáticos específicos, como forma de conservar para que futuramente sejam utilizados como prova (MINTO, 2021). A importância desse meio se mostra frente a volatilidade dos dados digitais, permitindo o armazenamento apropriado antes que se percam ou sejam adulterados e assim, posteriormente possam ser utilizados de forma efetiva.

O segundo meio, que está no artigo 18, trata-se da ordem de produção, ou injunção. Que diz respeito à permissão que os Estados signatários têm de “ordenar” a apresentação ou entrega de dados informáticos a qualquer ente ou terceiros que tenha posse destes (MINTO, 2021, p. 38). Está diretamente relacionada à apreensão dos dados, de forma a permitir que o ente estatal consiga formar um banco de dados para o uso devido em suas investigações.

O terceiro meio, previsto no artigo 19, trata da busca e apreensão de dados informáticos, em que os Estados mediante a adoção de medidas legislativas habilitarão suas autoridades competentes a proceder às buscas de sistemas ou suportes informáticos (MINTO, 2021). Diferentemente do meio anterior, esse, por sua vez, pretende a apreensão dos dados sem qualquer comunicação com quem o tenha sob seu domínio.

Por fim, o quarto e último meio, previsto nos artigos 20 e 21, trata da coleta em tempo real de dados informáticos, ou interceptação dos dados ao tempo em que estão sendo produzidos. Aqui, pretende-se obter informações no meio de uma transmissão de dados e não entre dados já armazenados previamente (MINTO, 2021). Essa divisão se coaduna com a posição de Kerr (2005, p. 285), para quem:

O processo de coleta de evidências eletrônicas em casos de hacking de computador geralmente se divide em três etapas. Começa com a coleta de evidências armazenadas em servidores de terceiros, segue para a vigilância prospectiva e termina com a investigação forense do computador do suspeito. Essas três etapas abrangem os mecanismos básicos da coleta de evidências digitais: coleta de evidências digitais em trânsito, coleta de evidências digitais armazenadas com terceiros amigáveis e coleta de evidências digitais armazenadas com partes hostis, como o alvo. Cada mecanismo apresenta fatos únicos e requer considerações especiais.

No que se referem as normativas nacionais há pelo menos quatro diplomas legais que fazem referência a obtenção de provas digitais que merecem uma breve análise. O primeiro

seria a Lei 9.296/96 (Lei de Interceptação de Comunicações Telefônicas, Interceptações Telemáticas e Captação Ambiental), que em seu primeiro artigo já direciona sua aplicabilidade em sistemas de informática e telemática. Essa lei tem como objetivo permitir o acesso a comunicações em trânsito, e em tempo real, muito próximo ao que prevê título 5, da Seção 2, da Convenção de Budapeste. Entretanto, como a própria lei expõe, trata-se de um mecanismo excepcional a ser utilizado apenas na falta de outros meios para obtenção da prova.

O segundo diploma é o Marco Civil da Internet Lei 12.965/14, que possui em alguns artigos específicos sobre provas digitais relativos a guarda de informações e a disponibilização das mesmas (Artigos 10 e 13), e o requerimento por meio de ordem judicial de informações relativas a registros de conexão ou de registros de acesso a aplicações de internet, e assim formarem o conjunto probatório do processo (artigo 22). Disposições também próximas aos títulos 2 e 3 da Convenção de Budapeste.

Os dois últimos diplomas são a Lei 8.069/90 (Estatuto da Criança e do Adolescente - ECA) e a Lei 12.850 (Lei das Organizações Criminosas), que apesar de positivarem questões distintas, em relação a provas digitais tratam de Infiltração Virtual. Ocorre em ambas as situações a utilização desse meio de prova está submetido a requisitos relacionados a autorização judicial, prazo de realização e entrega de todas as informações relativas a atividade de infiltração a ser realizada, além da excepcionalidade de sua aplicação.

Do exposto se extrai que as provas digitais têm sido tratadas de forma muito tímida no Brasil, com disposições para questões específicas e crimes pré-estabelecidos, além de serem tratadas de forma excepcional e estarem submetidas a requisitos e regras de aplicação com certo grau de exigência. Dessa forma não há ainda condições normativas suficientes que direcionem ou até mesmo impulsionem a utilização das provas digitais automatizadas.

6.2 Conformidade Ética das Provas Digitais Automatizadas

Para além da conformidade legal, é necessário dispor de balizas éticas para as provas digitais, especialmente no contexto de sistemas de IA. As provas automatizadas trazem também uma carga ética que merece atenção, no que diz respeito aos princípios que devem ser levados em consideração para que sejam efetivamente aplicadas, uma vez que a Inteligência Artificial pode dar margem para uma série de questionamentos e riscos que podem ir de encontro as garantias e direitos fundamentais de um indivíduo. Como consectário da utilização de inteligência artificial para construção e funcionamento da prova digital, é necessário dispor acerca de ditames éticos que estabeleçam balizas para o seu desenvolvimento.

As provas digitais, nesse cenário, precisam estar alinhadas a um design humanístico, na esteira do “*human centered design*”, de forma que haja o dimensionamento da função deferida à tecnologia seja influenciada por diretrizes que preservem e promova a dignidade da pessoa humana, especialmente a partir do desenvolvimento de princípios éticos (MULHOLLAND; FRAJHOF, 2021). A ética aplicada aos sistemas de IA, a seu turno, busca construir princípios que orientam o desenvolvimento do maquinário inteligente, bem como a sua capacidade de chegar a resultados que respeitem dados valores do ambiente sociocultural contemporâneo (BARTNECK et al, 2021).

Assim, Blackman (2022) endereça três principais desafios no uso de sistemas de inteligência artificial, que podem ser considerados eixos para construção de ditames éticos: (i) privacidade, isto é a forma como o aprendizado de máquina observa as normas de privacidade digital e uso coerente de dados pessoais; (ii) explicabilidade; (iii) mitigação de vieses discriminatórios. Esses eixos se relacionam diretamente com a necessidade de o sistema não criar resultados discriminatórios ou incorretos, na medida em que a utilização de IA para essa função representa um risco direto a direitos fundamentais (MENDES; MATTIUZZO, 2019; MAGALHÃES; GOMES, 2021).

Para fins do presente estudo é importante consignar que o conceito de discriminação – especialmente discriminação algorítmica – se correlaciona com a reverberação de práticas historicamente construídas de ordem de subjetivação de grupos de pessoas por fatores como cor da pele, origem étnico-racial, gênero, orientação sexual, ou qualquer forma de estigmatização (DUARTE, 2021). A discriminação, nesse contexto, não se relaciona com os termos “preconceito”, “estereótipo” ou “ideologia”, na medida em que aquela representa um comportamento, uma ação concreta, independentemente de vontade ou consciência (DUARTE, 2021). Dessa forma, a discriminação por uso de inteligência artificial pode não decorrer da subjetividade do programador, sendo possível decorrer da própria dinâmica de funcionamento ou do modelo de aprendizado implementado (BAROCA; SELBST, 2016).

Sob a ótica socio-legal dos riscos discriminatórios associados aos processos de aprendizado de máquina, Mendes e Mattiuzzo (2019) elencam quatro formas de produção de resultados injustos no seio social: (i) a partir de discriminação oriunda de falha no processamento do algoritmo; (ii) a partir da discriminação por conta do uso de dados sensíveis, levando em conta questões íntimas capazes de infirmar preconceitos, conscientes ou não, do programador; (iii) a partir da discriminação que resulte em limitação de direitos para os afetados; e (iv) a partir da discriminação por generalização, isto é, quando o sistema atribui,

diretamente ou através de *proxies*, características de um grupo a um certo indivíduo, desconsiderando suas particularidades.

Observando-se as diretrizes éticas dispostas em órgãos supranacionais, como a Organização para a Cooperação e Desenvolvimento Econômico – OCDE – e o Grupo Independente de Peritos de Alto Nível sobre a Inteligência Artificial – “GPAN IA” –, é possível consignar vetores deontológicos de maior aplicabilidade no contexto das provas digitais automatizadas. O GPAN IA erigiu os seguintes ditames éticos para o desenvolvimento de uma IA confiável: (i) respeito à autonomia humana; (ii) prevenção de danos; (iii) equidade; (iv) explicabilidade (COMISSÃO EUROPEIA, 2019). Por sua vez, a OCDE estabeleceu, em sua *Recommendation of the Council on Artificial Intelligence*, os seguintes princípios: (i) crescimento inclusivo; (ii) justiça e valores centrados no ser humano; (iii) transparência e explicabilidade; (iv) robustez, segurança e precaução; e (v) *accountability* ou responsabilidade (OCDE, 2019)

No presente estudo, põe-se em foco os princípios éticos de prevenção, transparência e responsabilidade, por observar um maior espaço de discussão no contexto das provas digitais, especialmente por haver uma correlação direta com a necessidade de mitigar os vieses, cujas consequências podem ser devastadoras no âmbito do processo penal (JESUS; MILAGRES, 2016; MAGALHÃES; GOMES, 2021). O princípio da prevenção se correlaciona com a necessidade de proteção da pessoa humana no tocante à sua dignidade e integridade física e mental contra utilizações maléficas, tendo-se em mente o risco de agravamento de assimetrias de poder (COMISSÃO EUROPEIA, 2019). Quanto às provas digitais, é importante destacar que o seu uso não pode reverberar preconceitos ou ter por consequência a ampliação de estruturas de subjetivação, sejam elas pautadas em discriminações por raça (COSTA; ACIOLY, 2022), por gênero (BETTEGA, 2021), ou qualquer outra forma.

Em relação à explicabilidade, é importante constatar que sua aplicação concerne ao controle social dos algoritmos de IA, e escrutínio público dos riscos discriminatórios, (MITTELSTADT et al, 2016). Ainda que não se busque tratar à exaustão da conceituação dos termos explicabilidade, interpretabilidade e compreensibilidade (PEREIRA, 2021; RUDIN, 2019), para fins do presente estudo, importa consignar a mera disponibilidade de informações, ainda que do código-fonte, não tem o condão de suprir a lacuna deixada pela inescrutabilidade das redes neurais artificiais, posto que a própria lógica dos algoritmos de aprendizado, de natureza adaptativa e autônoma, é um entrave à efetiva governança social (DUARTE, 2021).

O sentido e alcance do princípio da explicabilidade é dado pela necessidade de compreensibilidade e acessibilidade na resolução de problemas no caso concreto, mantendo-se

uma estrutura de confiança entre o usuário e o sistema IA (MITTELSTADT et al, 2016). Portanto, muito além de retórica argumentativa (BLACKMAN, 2022), a explicabilidade pode ser endereçada como um princípio que viabiliza a concretização de seus pares, o que dirige à sua materialização no caso concreto.

Para além destes vetores, é importante tecer como parâmetro ético o respeito à privacidade e à proteção de dados pessoais como supedâneo ao funcionamento das provas digitais. O direito de ser deixado só – *right to be left alone* (CANCELIER, 2017) – em períodos atuais pressupõe o controle informacional pelos próprios cidadãos, como medida de administração das próprias informações, afastando-se da noção de sigilo (OLIVEIRA, 2022). Não se pode olvidar que noção de privacidade como pressuposto ao livre desenvolvimento da personalidade, medida que se impõe para o alcance do livre proceder sem receio de julgamento sobre a vida privada (CANCELIER, 2017).

A partir da pesquisa empreendida, é possível observar o estabelecimento de parâmetros éticos ao uso de provas digitais automatizadas não se adstringem a essa forma de produção de evidências, mas decorrem de um conjunto de vetores de direcionamento do uso de tecnologias como Inteligência Artificial e regulação do fluxo informacional, de forma que tais eixos deontológicos não se mostram estáticos, mas submetidos à dinâmica evolutivo dos estudos das respectivas áreas.

7 CONCLUSÃO

Diante do exposto, é possível compreender que o uso de provas digitais é uma realidade intrínseca do contexto social vivido, que está imerso no uso constante de tecnologia e a conseqüente elevada produção de dados em todo momento. Inevitavelmente, o uso das evidências produzidas no e pelo contexto digital iriam atingir a realidade processual, com a inclusão de provas digitais para composição do processo, uma vez que boa parte das questões ocorrem quase que completamente no ambiente online.

A prova digital se enquadra como um meio de prova atípico, que apesar de suas particularidades, tem a contribuir não apenas com a condução processual objetiva do processo, como também a preservação do exercício do direito fundamental à prova das partes. Já que há casos em que a única prova disponível é a digital e esta não deve ser preterida, se for legal, suprir as necessidades processuais e for efetivamente apta para provar os fatos.

Diferentemente dos meios tradicionais de prova, a prova digital tem peculiaridades relevantes, que devem ser levadas em consideração mediante seu uso, para que consiga manter

as características suficientes de uma prova válida e apta ao uso no processo. A evidência a essas características, imaterialidade, volatilidade ou fragilidade e facilidade de dispersão, possibilitará que seja mantido minimamente os direitos dos indivíduos, já que a utilização indiscriminada pode levar a arbitrariedades.

Somadas às questões apresentadas está a introdução da Inteligência Artificial. Uma vez que grande parte dos processos cotidianos incorrem em manejo direto ou indireto de sistemas pautados em *machine learning*, observou-se a sua introdução em circunstâncias processuais, panorama denominado de provas digitais automatizadas. Nesse contexto, a máquina não apenas é capaz de armazenar evidências, mas de uni-las para formação de um elemento de prova. A questão é que a Inteligência Artificial, além de representar um campo de estudo ainda em desenvolvimento, na qual se destaca o risco de imprevisibilidade e ausência de completo domínio sobre os seus efeitos, ela está sendo aplicada no campo das provas digitais, que paralelamente encontra-se em desenvolvimento, carente de normativas sedimentadas. Observou-se não somente problemáticas e preocupações de matéria eminentemente jurídicas, mas também quesitos éticos.

No que se refere à consolidação normativa das provas digitais automatizadas, observou-se a necessidade de uma padronização do conceito e regime jurídico das provas digitais em si, como etapa preliminar à inclusão das nuances em torno da Inteligência Artificial. Apesar da existência de alguns dispositivos normativos que se referem às provas digitais, eles ainda direcionam o seu uso para a esfera da excepcionalidade e não são capazes de abarcar a latência social que representa o seu uso cotidiano, demonstrando um descolamento social que representa um claro caso de lacuna fática do direito (SOARES, 2016).

Em relação a ética, observou-se que, face a presença contínua da IA no cotidiano social, não se pode ignorar suas consequências, de forma que princípios devem delinear o uso devido da máquina, sem que gere a intrusão as garantias e direitos fundamentais. Tais princípios tem o condão de fornecer estruturas robustas de ética digital, consolidando proposituras de governança, dando-lhes sentido e alcance, especialmente na proteção de direitos fundamentais dos possíveis afetados.

Assim, a utilização de provas digitais com influência de mecanismos de inteligência artificiais deve ser pautada por um conjunto ético-normativo, essencialmente relacionados à privacidade, explicabilidade e mitigação de vieses, que sejam coerentes com o estado da arte sobre ética no uso e desenvolvimento de IA, a partir de influxos de coordenação com as normas esparsas que tem o potencial de disciplinar o uso de provas digitais. O contexto da transformação do Poder Judiciário brasileiro, consentâneo ao movimento de Justiça 4.0, deve

ser balizado com a aplicação no processo penal de provas digitais automatizadas, geradas a partir de um panorama ético que garanta a sua eficácia e legitimidade.

REFERÊNCIAS

- ACIOLY, Luis Henrique de Menezes. A aplicação do Princípio da Função Social do Contrato em Contratos Eletrônicos de redes sociais e seu papel na democratização de Direitos Fundamentais. In: **Conversas Civilísticas**, Salvador, v. 1, n. 2, p. 111-134, jul./dez. 2021. Disponível em: <https://periodicos.ufba.br/index.php/conversascivilisticas/article/view/47143>. Acesso em: 03 ago. 2022.
- ALBINO, João Pedro; LIMA, Ana Cláudia Pires Ferreira. Inteligência Artificial utilizada para garantir direitos. In: ALBINO, João Pedro; VALENTE, Vânia Cristina Pires (orgs.). **Inteligência Artificial e suas aplicações interdisciplinares**. Rio de Janeiro: e-Publicar, 2023, p. 35-57.
- ARAÚJO, Valter Shuenquener; GABRIEL, Anderson de Paiva; PORTO, Fábio Ribeiro. Justiça 4.0: a transformação tecnológica do poder judiciário deflagrada pelo CNJ no biênio 2020-2022. In: **Revista Eletrônica Direito Exponencial**. v. 1, n. 1, 2022, p. 1-18. Disponível em: <<https://doi.org/10.22477/diex.v1i1.796>>. Acesso em: 11 set. 2023.
- BAROCAS, Solon; SELBST, Andrew. Big Data's Disparate Impact. In: **California Law Review**, v. 104, 2016, p. 671-732. Disponível em: <<http://dx.doi.org/10.2139/ssrn.2477899>>. Acesso em: 28 jun. 2023.
- BARTNECK, Christoph; LUTGE, Christoph; WAGNER, Alan; WELSH, Sean. **An Introduction to Ethics in Robotics and AI**. Cham: Springer Switzerland, 2021.
- BETTEGA, Elisa. O que fazer sobre o viés algorítmico baseado em gênero?. In: BARBOSA, Bia; TRESKA, Laura; LAUSCHNER, Tanara (orgs.). **Governança da Internet e Gênero: tendências e desafios**. [s.l.]:CGI.Br., 2021. p. 125-133.
- BLACKMAN, Reid. **Ethical Machines: Your Concise Guide to Totally Unbiased, Transparent, and Respectful AI**. Boston: Harvard Business Review Press, 2022.
- CANCELIER, Mikhail Vieira de Lorenzi. O Direito à Privacidade hoje: perspectiva histórica e o cenário brasileiro. In: **Seqüência (Florianópolis)**, n. 76, ago. 2017, p. 213-240. Disponível em: <<https://doi.org/10.5007/2177-7055.2017v38n76p213>>. Acesso em: 03 jan. 2023.
- CAPEZ, Fernando. **Curso de processo penal**. 30. ed. São Paulo: Saraiva, 2023.
- CARVALHO, Tiago Jose de; PEDRINI, Helio; ROCHA, Anderson de Rezende. Visual Computing and Machine Learning Techniques for Digital Forensics. In: **Revista de Informática Teórica e Aplicada**, v. 22, n. 1, p. 128–153, 2015. DOI: 10.22456/2175-2745.49492. Disponível em: <https://seer.ufrgs.br/index.php/rita/article/view/RITA-VOL22-NR1-128>. Acesso em: 26 ago. 2023.
- CASEY, Eoghan. **Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet**. 3. ed. Baltimore: Academic Press, 2011.

CASTELLS, Manuel. **A sociedade em rede**. Trad. Roneide Venâncio Majer. 6. ed. São Paulo: Paz e Terra, 2002.

CASTIGLIONE, Aniello; CATTANEO, Giuseppe; DE MAIO, Giancarlo; DE SANTIS, Alfredo. Automated Production of Predetermined Digital Evidence. In: **IEEE Access**, v. 1, p. 216-231, 2013. Disponível em: <https://ieeexplore.ieee.org/document/6514969>. Acesso em 22 ago. 2023.

COMISSÃO EUROPEIA. **Orientações éticas para uma IA de confiança**. Publications Office, 2019. Disponível em: <<https://data.europa.eu/doi/10.2759/2686>>. Acesso em: 15 jul. 2023.

COSTA, Jéssica Hind Ribeiro; ACIOLY, Luis Henrique de Menezes Acioly. Discriminação Racial e Inteligência Artificial: Caminhos Possíveis à Plena Cidadania Virtual. In: MACEDO, Humberto Gomes; BENTES, Dorinthe dos Santos; ANDRADE, Pedro Gustavo Gomes (coord.). **Os direitos humanos na era tecnológica III**. III Congresso Internacional de Direito e Inteligência Artificial (III CIDIA). Belo Horizonte: Skema Business School, 2022, p. 53-60.

DUARTE, ALAN. **A Antidiscriminação no contexto da inteligência artificial**: possibilidades de governança mediante a normatização de algoritmos. Fortaleza: Mucuripe, 2021.

FERNANDES, Antonio Scarance; ALMEIDA, José Raulgo Gustavo de; MORAES, Maurício Zanoide de. **Provas no Processo Penal**: estudo comparado. São Paulo: Saraiva, 2011.

FONSECA, Edson Pires. **Lei Geral de Proteção de Dados Pessoais**. 2. ed. Salvador: JusPodivm, 2022.

FORD, Martin. **Rule of the Robots**: how artificial intelligence will transform everything. New York: Basic Books, 2021.

GUSTIN, Miracy Barbosa de Sousa; DIAS, Maria Tereza Fonseca; NICÁCIO, Camila Silva. **(Re) pensando a pesquisa jurídica**: teoria e prática. 5. ed. rev., ampl. e atual. São Paulo: Almedina Brasil, 2020.

HASSAN, Nihad. **Digital Forensics Basics**: a practical guide using windows OS. New York: Apress, 2019.

IRONS, Alastair; LALLIE, Harjinder Singh. Digital forensics to intelligent forensics. In: **Future Internet**, v. 6, n. 3, p. 584-596, 2014.

JENKINS, Henry. **Cultura de Convergência**. Trad. Susana Alexandria. 2. ed. ampl. e atual. São Paulo: Aleph, 2009.

JESUS, Damásio de; MILAGRE, José Antonio. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016.

LARONGA, Antonio. **Le prove atipiche nel processo penale**. Milão: CEDAM, 2002.

LEE, Kai-Fu. **Inteligência artificial**: como os robôs estão mudando o mundo, a forma como amamos, nos relacionamos, trabalhamos e vivemos. Trad. Marcelo Barbão. Rio de Janeiro: Globo Livros, 2019.

LÉVY, Pierre. **O que é o virtual?**. São Paulo: 34, 1996.

LOPES JÚNIOR, Aury. **Direito Processual Penal**. 18. ed. São Paulo: Saraiva, 2021.

LUO, Xinkai. Blockchain como novo veículo da prova digital, uma experiência chinesa. In: **Revista Acadêmica da Faculdade de Direito do Recife**, v. 94, n. 2, 2022, p. 26-49. Disponível em: <https://doi.org/10.51359/2448-2307.2022.253028>. Acesso em: 26 ago. 2023.

LUPÁRIA, Luca. La disciplina processuale e le garanzie difensive. In: LUPÁRIA, LUCA; ZICCARDI, Giovanni (orgs). **Investigazione penale e tecnologia informatica**: L'accertamento del reato tra progresso scientifico e garanzie fondamentali. Milão: Guiffirè, 2007.

MADALENA, Juliano. Regulação das Fronteiras da Internet: um primeiro passo para uma Teoria Geral do Direito Digital. In: MARTINS, G. M.; LONGHI, J. V. R. (coords.). **Direito Digital: Direito Privado e Internet**. 2. ed. Indaiatuba: Foco, 2019. p. 183-206.

MAGALHÃES, Alice Azevedo; GOMES, Tércio Spínola. Regulação de sistemas de reconhecimento facial para fins de segurança pública no brasil: riscos e desafios. In: **Revista Humanidades e Inovação**. v. 8, n. 47, 2021, p. 168-182. Disponível em: <<https://revista.unitins.br/index.php/humanidadeseinovacao/article/view/5639>>. Acesso em: 15 jul. 2023.

MARQUES, João Alexandre Lobo. Computação forense e inteligência artificial. In: MONTEIRO, Marcos (org.). **Informática Forense**. Coleção Tratado de Perícias Forenses. São Paulo: Leud, 2018, p. 389-424.

MAZIEIRO, Carlos Alberto. **Sistemas operacionais**: conceitos e mecanismos. Curitiba: DINF - UFPR, 2019.

MENDES, Laura Schertel; MATTIUZZO, Marcela. Discriminação Algorítmica: Conceito, Fundamento Legal e Tipologia. **RDU**, Porto Alegre, v. 16, n. 90, p. 39-64, nov-dez 2019. Disponível em: <<https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3766>>. Acesso em: 02 jul. 2023.

MINTO, Andressa Olmedo. **A Prova Digital no Processo Penal**. São Paulo: LiberArs, 2021.

MITTELSTADT, Brent Daniel; ALLO, Patrick; TADDEO, Mariarosaria; WACHTER, Sandra; FLORIDI, Luciano. The ethics of algorithms: Mapping the debate. In: **Big Data & Society**. v. 3, n. 2, jul./dez., 2016, p. 1-21. Disponível em: <<https://doi.org/10.1177/2053951716679679>>. Acesso em: 23 jul. 2023.

MULHOLLAND, Caitlin; FRAJHOF, Isabella. Entre as leis da robótica e a ética: regulação para o adequado desenvolvimento da inteligência artificial. In: BARBOSA, Mafalda Miranda; BRAGA NETTO, Felipe; SILVA, Menezes Cordeiro; FALEIROS JÚNIOR, José Luiz Moura. (coords.). **Direito Digital e Inteligência Artificial**: Diálogos entre Brasil e Europa. Indaiatuba: Foco, 2021, p. 65-80.

OLIVEIRA, Manuela. **A aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) nos cartórios extrajudiciais**: uma análise acerca da expedição de certidões em ofícios de registro de imóveis da Bahia. Orientador: Maurício Requião Sant'Anna. 2022, 88 f. il.

Monografia – Faculdade de Direito, Universidade Federal da Bahia, Salvador, 2022.
Disponível em: <<https://repositorio.ufba.br/handle/ri/36291>>. Acesso em: 03 jan. 2023.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT.
Recommendation of the Council on Artificial Intelligence (OECD/LEGAL/0449). Paris: OECD, 2019.

PACELLI, Eugênio. **Curso de Processo Penal**. 27. ed. Salvador: JusPodivm, 2023.

PADILHA, Rafael; THEÓPHILO, Antônio; ANDALÓ, Fernanda; VEGA-OLIVEROS, Didier; CARDENUTO, João; BERTOCCO, Gabriel; NASCIMENTO, José; YANG, Jing; ROCHA, Anderson. A Inteligência Artificial e os desafios da Ciência Forense Digital no século XXI. In: **Estudos Avançados**, v. 35, n. 101, jan./abr. 2021, p. 111-138. Disponível em: <<https://doi.org/10.1590/s0103-4014.2021.35101.009>>. Acesso em: 14 ago. 2023.

RAMPIM, Talita; IGREJA, Rebecca Lemos. Acesso à Justiça e Transformação Digital: um Estudo sobre o Programa Justiça 4.0 e Seu Impacto na Prestação Jurisdicional. In: **Revista Direito Público**, v. 19, n. 102, 2022. Disponível: <<https://doi.org/10.11117/rdp.v19i102.6512>>. Acesso em: 11 set. 2023.

SAXENA, Ishi, USHA, G, VINOOTH, N.A.S., VEENA, S. e NANCY, Maria. The Future of Artificial Intelligence in Digital Forensics: A Revolutionary Approach. In: Karthikeyan, P.; PANDE, Hari Mohan; Sarveshwaran, Velliangiri (eds.) **Artificial Intelligence and Blockchain in Digital Forensics**. River Publishers, 2023.

SCHWAB, Klaus. **A quarta revolução industrial**. São Paulo: Edipro, 2019.

SILVA FILHO, Wilson. Crimes Cibernéticos e Computação Forense. In: XVI Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais. 2016. Niterói. **Anais**. Niterói: Sociedade Brasileira de Computação, 2016, p. 44-78.

SOARES, Ricardo Maurício Freire. **Elementos de Teoria Geral do Direito**. 3. Ed. atual., rev. e ampl. São Paulo: Saraiva. 2016.

TAUK, Caroline Somesom; SALOMÃO, Luis Felipe. Inteligência Artificial no Judiciário Brasileiro: Estudo Empírico sobre algoritmos e discriminação. In: **Diké (Uesc)**, v. 22, n 23, p. 02-32, jan./jun. 2023. Disponível em: <<https://doi.org/10.36113/dike.23.2023.3819>>. Acesso em: 11 set. 2023.

TÁVORA, Nestor; ALENCAR, Rosmar Rodrigues. **Curso de Processo Penal e Execução Penal**. 17. ed. Salvador: JusPodivm, 2022.

THAMAY, Rennan; TAMER, Maurício. **Provas no Direito Digital: Conceito da Prova Digital, Procedimentos e Provas Digitais em espécie**. São Paulo: Revista dos Tribunais, 2022.

VAZ, Denise Provasi. **Provas digitais no processo penal: formulação do conceito, definição das características e sistematização do procedimento probatório**. 198 f. 2012. Tese (Doutorado em Direito Processual) - Faculdade de Direito, Universidade de São Paulo, São Paulo, 2012. Disponível em: <https://www.teses.usp.br/teses/disponiveis/2/2137/tde-28052013-153123/pt-br.php>. Acesso em: 22 ago. 2023.