UNIVERSIDADE FEDERAL DO CEARÁ

FACULDADE DE DIREITO

PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO

Área de Concentração em Constituição, Sociedade e Pensamento Jurídico

ISABELLE BRITO BEZERRA MENDES

A ADMISSIBILIDADE DA PROVA DIGITAL AUTOMATIZADA NO SISTEMA PROCESSUAL BRASILEIRO: JUSTEZA ÉTICO-NORMATIVA NO USO DE INTELIGÊNCIA ARTIFICIAL NA PRODUÇÃO DE PROVAS.

Fortaleza

2024

ISABELLE BRITO BEZERRA MENDES

A ADMISSIBILIDADE DA PROVA DIGITAL AUTOMATIZADA NO SISTEMA PROCESSUAL BRASILEIRO: JUSTEZA ÉTICO-NORMATIVA NO USO DE INTELIGÊNCIA ARTIFICIAL NA PRODUÇÃO DE PROVAS.

Dissertação apresentada ao Programa de Pós-Graduação em Direito da Universidade Federal do Ceará, como requisito parcial à obtenção do título de Mestre em Direito Constitucional. Área de concentração: Direitos Fundamentais e Políticas Públicas.
Orientador: Prof. Dr. Maria Vital da Rocha.
Co-orientador: Prof. Dr. João Araújo Monteiro Neto

Fortaleza
2024

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Sistema de Bibliotecas
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

M491a Mendes, Isabelle.
A ADMISSIBILIDADE DA PROVA DIGITAL AUTOMATIZADA NO SISTEMA PROCESSUAL BRASILEIRO: JUSTEZA ÉTICO-NORMATIVA NO USO DE INTELIGÊNCIA ARTIFICIAL NA PRODUÇÃO DE PROVAS. / Isabelle Mendes. – 2023.
88 f.

Dissertação (mestrado) – Universidade Federal do Ceará, Faculdade de Direito, Programa de Pós-Graduação em Direito, Fortaleza, 2023.
Orientação: Prof. Dr. Maria Vital da Rocha.
Coorientação: Prof. Dr. João Araújo Monteiro Neto.

1. Prova Digital. 2. Prova Digital Automatizada. 3. Inteligência Artificial. 4. Cadeia de Custódia. 5. Devido Processo Legal. I. Título.

CDD 340

ISABELLE BRITO BEZERRA MENDES

A ADMISSIBILIDADE DA PROVA DIGITAL AUTOMATIZADA NO SISTEMA PROCESSUAL BRASILEIRO: JUSTEZA ÉTICO-NORMATIVA NO USO DE INTELIGÊNCIA ARTIFICIAL NA PRODUÇÃO DE PROVAS.

Dissertação apresentada ao Programa de Pós-Graduação em Direito da Universidade Federal do Ceará, como requisito parcial à obtenção do título de Mestre em Direito Constitucional. Área de concentração: Direitos Fundamentais e Políticas Públicas.

Aprovada em: 20/02/2024.

BANCA EXAMINADORA

_____

Prof. Dr. Maria Vital da Rocha (Orientador)
Universidade Federal do Ceará (UFC)

_____

Prof. Dr. João Luís Nogueira Matias
Universidade Federal do Ceará (UFC)

_____

Prof. Dr. João Araújo Monteiro Neto
Universidade de Fortaleza (Unifor)

A Deus. Que por sua bondade me permitiu chegar até aqui.
E aos meus pais, Alexandre e Léa, que são minhas grandes inspirações acadêmicas, e que nunca mediram esforços para apoiar meus sonhos.

AGRADECIMENTOS

Certo é que não se chega a canto nenhum sozinho, nem mesmo é possível tornar-se o que se sonha de forma independente e autônoma. Dessa forma, reconhecer quem de alguma forma nos ajudou a chegar até aqui é coerente e necessário.

Inicialmente quero agradecer a Deus, que tem sido fiel em todo tempo e me permitiu cursar o mestrado, um sonho grande desde a época da graduação. Esta é mais uma demonstração de Sua infinita bondade e graça.

A minha professora orientadora Maria Vital, a qual tenho profundo respeito e admiração, que acreditou em meu potencial desde o primeiro dia e tem me motivado a persistir na vida acadêmica e acreditar que ainda alcançarei os sonhos grandes que estão em mim.

Ao meu professor co-orientador, que já me acompanha desde a graduação e tem sido um grande mestre acadêmico para mim. Sou grata por todo incentivo que me deu nesses dois anos, confiando em meu trabalho, mas também me direcionando para oportunidades relevantes na minha jornada acadêmica.

Aos meus pais, por acreditarem e investirem em mim com tanto afinco e carinho. Sem vocês efetivamente não teria chegado até aqui. Obrigada, pelas portas abertas, pelo acompanhamento diário e pelas orações pela minha vida.

A minha irmã querida, por todas as palavras de incentivo e por achar que sou mais inteligente que ela, mas a verdade é que seu esforço me inspira.

A minha amiga Camila Oliveira, que não entende metade das minhas conversas relativas a Inteligência Artificial, Direito Digital, Privacidade e Proteção de Dados, mas diz que tem orgulho de mim e me suporta no meio dos meus desafios acadêmicos desde a graduação, além de ajudar a padronizar todas as minhas referências.

Aos meus amigos do GETIS, Luís Henrique Acioly e Matheus Fernandes, companheiros de pesquisas, artigos e apresentações. Obrigada por toda parceria acadêmica nesses dois anos, pela amizade firme mesmo em dias que não queremos escrever uma linha e por tanto me ensinarem. E as amigas Larissa Nunes e Narllyane Guedes que me incentivam todos os dias com muita paciência e carinho, além de serem auxílio essencial nos meus dias corridos.

Aos amigos Ricardo Maia e Ana Paula Buosi, que foram grandes inspirações para mim no processo de mestrado, dispendendo ajuda generosa no decorrer dos dias, desde o processo seletivo, até o desenvolvimento da pesquisa.

A minha conselheira Jessica, que abriu as portas no meu trabalho, com muito esforço e comprometimento, para que conseguisse conciliar da melhor forma as demandas advindas dessas duas áreas importantes da minha vida, e por acreditar sempre no meu potencial, tirando o melhor de mim.

Por fim, agradeço aos amigos próximos e queridos, tanto aos que estão aqui há muito tempo, como aqueles que há pouco chegaram, mas já se fazem relevantes, que me apoiaram nessa etapa e que de alguma forma ajudaram durante o processo, contribuindo também para que esse resultado fosse possível.

“E na ciência e tecnologia? Sim, avançamos; sim, fizemos máquinas voadoras. Conectamos nossos computadores uns aos outros; mas será que isso truxe paz ao coração humano? Será que resolveu a nossa dor? Ou apenas proveu novos canais para falarmos da mesma dor? Além de criar dores novas é claro. E mesmo em nossas invenções tecnológicas, o que há de novo?” (GAROFALO NETO, 2020, p.55).

RESUMO

O presente trabalho tem como objetivo analisar a utilização da Inteligência Artificial (IA) no contexto da produção de prova digital. Uma vez que o uso de novas tecnologias já se encontra disseminado em todas as áreas da existência humana, não seria incoerente pensar que há ramificações diretas no contexto judiciário e processual. Por isso, é fundamental compreender como a tecnologia pode impactar no que diz respeito ao acesso à justiça e ao devido processo legal. Na esfera processual, as discussões sobre prova digital têm ganhado relevância, especialmente em matéria de legitimidade e validade jurídica. A inserção de ferramentas de inteligência artificial nesse contexto traz possibilidades relevantes e oportunidades, como a celeridade e a redução de gastos, por outro lado evidencia questões em torno da ética e da legalidade de sua utilização. Quais seriam então os padrões éticos-normativos mínimos que a jurisdição brasileira precisa estar submetida para que a utilização da produção probatória automatizada seja legal e fiável? É precisamente essa a pergunta principal que o presente trabalho visa responder. A pesquisa busca delinear os parâmetros para o uso da inteligência artificial na produção de provas digitais, com vistas a ponderar sua legitimidade e proteção de direitos fundamentais, com precisão, no contexto social da digitalização da vida no Brasil. Na primeira parte há uma análise sobre o direito constitucional a prova, bem como uma distinção conceitual entre prova e evidência. Na segunda e terceira partes o estudo se direciona em torno da prova digital, seus usos no contexto jurídico brasileiro, bem como a inserção e utilização da Inteligência Artificial nesta matéria. A última parte trata dos padrões mínimos que devem ser levados em conta, tais como os princípios da justiça, transparência, explicabilidade, responsabilidade, além do direcionamento normativo brasileiro no que se refere as provas digitais automatizadas. O trabalho então, busca contribuir para a proposição de aderência a padrões mínimos de ética e de direito, que a Inteligência Artificial requer para que esteja apta a ser utilizada na produção de provas sem contrariar direitos fundamentais. Metodologicamente, o trabalho propõe uma análise bibliográfica, através do método dedutivo, com o objetivo de compreender as repercussões sociais, jurídicas e internacionais do estudo - o que será feito através da leitura de livros, artigos, publicações, revistas e periódicos.

Palavras-chave: Prova Digital. Prova Digital Automatizada. Inteligência Artificial. Cadeia de Custódia. Devido Processo Legal. Acesso à Justiça.

ABSTRACT

This paper aims to analyze the use of Artificial Intelligence (AI) in the context of digital evidence production. Since the use of new technologies is already widespread in all areas of human existence, it would not be inconsistent to think that there are direct ramifications in the judicial and procedural context. It is therefore essential to understand how technology can impact on access to justice and due process of law. In the procedural sphere, discussions about digital evidence have gained relevance, especially in terms of legitimacy and legal validity. The inclusion of artificial intelligence tools in this context brings relevant possibilities and opportunities, such as speed and cost savings, but on the other hand raises questions about the ethics and legality of their use. So what are the minimum ethical and normative standards that Brazilian courts need to be subject to in order for the use of automated evidence production to be legal and reliable? This is precisely the main question that this paper aims to answer. The research seeks to outline the parameters for the use of artificial intelligence in the production of digital evidence, with a view to weighing up its legitimacy and the protection of fundamental rights, precisely in the social context of the digitalization of life in Brazil. In the first part there is an analysis of the constitutional right to evidence, as well as a conceptual distinction between evidence and proof. In the second and third parts, the study focuses on digital evidence, its uses in the Brazilian legal context, as well as the insertion and use of Artificial Intelligence in this area. The last part deals with the minimum standards that should be taken into account, such as the principles of fairness, transparency, explainability, responsibility, as well as the Brazilian regulatory framework with regard to automated digital evidence. The work then seeks to contribute to proposing adherence to minimum standards of ethics and law, which Artificial Intelligence requires in order to be able to be used in the production of evidence without contradicting fundamental rights. Methodologically, the work proposes a bibliographical analysis, using the deductive method, with the aim of understanding the social, legal and international repercussions of the study - which will be done by reading books, articles, publications, magazines and journals.

Keywords: Digital Evidence. Automated Digital Evidence. Artificial Intelligence. Chain of Custody. Due Process of Law. Access to Justice.

SUMÁRIO

1 INTRODUÇÃO

Não há mais como estudar o desdobramento das atividades sociais atuais sem levar em consideração a influência da tecnologia e o avanço científico. A posição intrínseca que a tecnologia ocupa no cotidiano humano, gerando mudanças e alterações no estado das coisas, pressiona o direito e o sistema jurídico por soluções e respostas que abarquem essas novidades e sejam adequadas a manutenção dos direitos e garantia fundamentais.

A facilitação gradual do acesso a determinadas ferramentas e aplicações digitais, bem como o progresso significativo dos equipamentos e técnicas computacionais, fez com que a produção de dados aumentasse significativamente, de forma que pela quantidade de dados produzida, pode-se obter informações relevantes e diversas sobre qualquer situação ou indivíduo mediante uma efetiva análise ou cruzamento de informações.

Todo esse processo permitiu o significativo desenvolvimento da Inteligência Artificial nos últimos trinta anos, de forma que experimentos que nos anos 50 não puderam ser continuados devido à falta de dados amostrais para o treinamento de uma máquina, hoje são efetivados com uma facilidade inexplicável, além de permitir o aumento de pesquisas e trabalhos científicos que geram cada vez mais ferramentas e possibilidades ainda mais avançadas, ampliando o espectro de aplicação dos sistemas de IA.

Frente a essa realidade, a Inteligência Artificial está presente nos mais diversos setores sociais, sendo quase que imperceptível na entrega de diversos serviços e na produção dos mais variados produtos. Essa realidade leva pouco a pouco a normalização de sua aplicação e o costume de seu uso, sem a preocupação consciente das consequências que pode gerar. Estas por sua vez acabam por se tornar perceptíveis apenas em razão do enfretamento de alguma problemática de difícil solução ou de consequências irremediáveis, as quais o direito muitas vezes munido de normativas desatualizadas nem mesmo tem condições de abarcar. O que leva a um imbróglio cíclico e interminável em que o avanço tecnológico continua a passos largos, o direito não prevenido não consegue abarcar e as dificuldades seguem ocorrendo sem o amparo legal devido, uma vez que a tecnologia continuará avançando.

Tendo como base essa perspectiva, e compreendendo que a Inteligência Artificial já está presente nas atividades jurídicas, plantando raízes cada vais mais sólidas e ramificando-se em quase todas as matérias jurisdicionais, entende-se que é necessário antecipar as discussões acadêmicas para que se consiga prever e compreender melhor as novas situações advindas dessa

dispersão tecnológica e de alguma forma desenvolver soluções. Por isso, esse trabalho visa discutir a aplicação de inteligência artificial no contexto da produção da prova digital, consciente de que não há muitas discussões sobre esse tema, mas certo de que sua aplicação já acontece no contexto jurídico e que é uma questão de poucos anos, ou meses, para que seja recorrente.

Uma vez que a prova é um mecanismo jurídico de entrega de um devido processo legal e consequentemente da manutenção de um direito constitucional de dispor do contraditório e da ampla defesa, possibilitar formas diversas para que esse direito se concretize é tarefa do direito. Inclusive, amoldando-se a realidade da cidadania digital em que vivemos, onde boa parte das relações interpessoais tem ocorrido online. A busca por provas digitais então tem aumentado significativamente, gerando inclusão no processo e pressionando o direito a abarcar essa realidade.

Ocorre que além da integração das provas digitais, tem-se aplicado mecanismos de automação da produção dessas provas por meio de Inteligência Artificial, uma vez que nem sempre o humano sozinho consegue chegar à prova, em razão da quantidade significativa de dados que precisam ser analisados em um prazo curto e a falta do aporte econômico necessário. Assim, a Inteligência Artificial se apresenta como uma solução viável, não somente para viabilizar a economia de tempo e dinheiro, como também para prover soluções a situações que de outra maneira seriam de difícil resolução e assim possibilitar a entrega de um processo devido.

Entretanto, essa aplicação não pode ocorrer de maneira desordenada, uma vez que a inclusão da prova, de uma forma geral, no processo requer toda uma cadeia de custódia, autorização normativa e jurisdicional para que seja considerada legal e apta para influenciar o livre convencimento do juiz. Não poderia ser diferente então com a prova digital automatizada. Ademais, não se pode desconsiderar as consequências da presença da Inteligência Artificial nessa situação, que pode gerar consequências negativas a continuidade da vida humana, devendo passar por uma análise precisa de sua adequação ética para que possa operar diretamente na vida dos indivíduos. Ou seja, esse tipo probatório proposto deve submeter-se a uma admissibilidade ética e normativa para que possa ser entranhado ao processo de forma legal e juridicamente coerente.

O presente trabalho então tem como objetivo geral compreender quais seriam os requisitos éticos e normativos os quais a prova digital automatizada deverá ser enquadrada para que possa ser efetivamente utilizada para prestação de um devido processo legal no contexto brasileiro. Especificamente buscar-se-a, compreender inicialmente o conceito de prova e como a prova digital automatizada pode se enquadrar a esse conceito, examinar a realidade brasileira de inclusão de provas no processo e o quanto esse processo é capaz de abarcar as provas digitais automatizadas, analisar a aplicação prática desse tipo probatório, e identificar as principais mudanças normativas que devem ser realizadas, bem como quais aspectos éticos devem ser levados em consideração para que a prova digital automatizada seja legalmente incluída ao processo e efetivamente utilizada.

A justificativa para esse trabalho está exatamente no impacto da tecnologia no direito, que não pode ficar inerte aos avanços conquistados e pode aproveitar-se das possibilidades digitais surgidas a seu favor para a garantia de direitos dos indivíduos, principalmente no que se referem entrega de um processo justo e equânime. Aqui há também que se mostrar que essa possibilidade não é de todo nova, levando em consideração a aplicação prática que já tem ocorrido, que também justifica a urgência da análise desse tema.

A metodologia utilizada no trabalho quanto a natureza se caracteriza como uma pesquisa bibliográfica, com a análise de livros, artigos, dissertações, e leis, com abordagem qualitativa buscando compreender o objeto em análise a partir da leitura de autores com domínio no assunto abordado, além da comparação com outros contextos. Trata-se de pesquisa descritiva, por indicar conceitos, situações e os cenários aplicáveis ao objeto, e exploratória, por buscar maiores informações sobre o tema abordado.

Na primeira parte desse trabalho, há uma breve compreensão do que seria o direito constitucional a prova, bem como a importância desse mecanismo processual para a entrega das garantias processuais e manutenção do acesso a justiça. Há também um esclarecimento sobre a diferença de prova e evidência, de forma a se desenvolver a compreensão do que efetivamente pode ser levado ao processo como meio capaz de influenciar do livre convencimento do juiz e o que seria mera informação crua sem ligação definitiva com o fato que se quer provar.

Na segunda parte há uma análise da questão probatória, até que se chegue a compreensão do que se trata a prova digital como se classificariam e como poderia ser aceita

no processo penal brasileiro como válidas. Destaca-se também a cadeia de custódia que a prova deveria passar para ser efetivamente entranhada ao processo, de forma a entender como a realidade brasileira tem absorvido essa realidade e quais são os pontos que precisam ser melhorados.

Na terceira parte há a definição do conceito de prova digital automatizada, como se aplica no contexto probatório e quais são as possibilidades positivas e negativas desse mecanismo. Há nesse capítulo também a disposição de casos práticos em que a provas digitais automatizada tem sido aplicada.

A última parte trata exatamente dos requisitos de admissibilidade ética, com a disposição de quatro princípios principais que devem ser levados em consideração quando se fala da inserção de inteligência artificial nos processos cotidianos. Bem como os requisitos de admissibilidade normativa, os quais o Brasil precisa adotar para que a prova digital automatizada seja legalmente autorizada e aplicável ao processo jurídico.

2 DIREITO À PROVA

Vive-se na era da informação, nunca tantos dados foram produzidos. O desenvolvimento rápido da tecnologia tem possibilitado não apenas a facilitação de processos e procedimentos, mas também a larga produção de informações sobre indivíduos, sociedades e serviços. É difícil identificar o que atualmente esteja longe de qualquer tipo de influência digital. Novas ferramentas e mecanismos surgem dia após dia, tornando cada vez mais difícil controlar esse alastramento digital.

A inteligência Artificial é elemento fundamental nesse contexto, uma vez que, ao longo da última década, tem dado saltos revolucionários e consequentemente fornecido um número cada vez maior de aplicações práticas que têm transformado significativamente as sociedades e o desenvolvimento das atividades humanas (Ford, 2021, p.3). E não é como se a Inteligência Artificial fosse uma matéria completamente nova e que apenas surgiu recentemente ganhando força. Na realidade, tem sido estudada há décadas, e seus princípios têm sido bem compreendidos esse tempo todo, mas os grandes saltos de desenvolvimentos recentes dessa matéria se deram por duas razões, conforme explica Martin Ford (2021, p.3): a primeira razão está exatamente na chegada de computadores muito mais poderosos que são ferramentas verdadeiramente capazes de realizar praticamente o que antes estava apenas no campo teórico. E a segunda razão está nos enormes tesouros de dados que estão sendo constantemente gerados e recolhidos em toda a economia da informação, sendo um recurso crucial para treinar as máquinas para a execução de tarefas úteis, e consequentemente o fator mais importante.

A disponibilidade de dados numa escala que outrora teria sido inimaginável é, sem dúvida, o fator mais importante subjacente ao progresso surpreendente que temos visto. Conforme Andrejevic (2017, p.75) explica, até a economia está cada vez mais dependente de dispositivos e plataformas digitais, que armazenam informações relativas a quase todas as esferas da existência social. A hipereficiência e a produtividade da vida contemporânea dependem da coleta e do processamento automatizado de dados. É o que Hintz, Dencik e Wahl-Jorgensen (2018, p.10) chamam de “capitalismo de dados”, que tem se tornado a base fundamental da sociedade contemporânea, sendo imprescindível para o bom funcionamento da economia e do Estado.

A dispersão cada vez maior de dispositivos móveis, softwares e atividades digitais, tem feito com que os indivíduos estejam cada vez mais inseridos no contexto digital, produzindo cada vez mais dados mediante suas interações com a tecnologia, seja apenas nas

atividades rotineiras de pesquisa e busca, como a interação intencional com aplicativos no celular que monitoram atividades ou requerem o upload de fotos e vídeos.

Essa relação intrínseca dos indivíduos com o digital tem pouco a pouco levado ao desenvolvimento de uma cidadania digital, na qual as atividades realizadas nesse contexto têm se tornado fundamentais não apenas para dar celeridade a vida, mas também, e principalmente, para a efetiva participação social (Hintz; Dencik; Wahl-Jorgensen, 2018, p.20). A conectividade digital tem também feito parte da construção social e política de sociedade. Os dados produzidos têm influenciado diretamente nos direcionamentos das comunidades.

Todas as interações realizadas têm sido mapeadas, fazendo com que se emerja uma nova dinâmica de poder entre os titulares dos dados (os cidadãos digitais) e aqueles que detêm, armazenam e controlam os dados (normalmente grandes empresas e os Estados). Nessa lógica, a constante transferência de dados e seu processamento tem possibilitado a compreensão, a predição e o controle das atividades dos indivíduos (Hintz, Dencik e Wahl-Jorgensen, 2018, p.37).

A informação por si só não é o que gera o desenvolvimento econômico, mas o processamento e organização dessa informação que posteriormente será transformado em conhecimento aplicado. Tem-se desenvolvido cada vez mais mecanismos, máquinas e softwares para o processamento desses dados, para que as informações a serem obtidas sejam efetivamente utilizadas. Destaca-se mais uma vez inserção da Inteligência Artificial, que tem sido largamente utilizada para o processamento dos dados, gerando decisões automatizadas que influenciam diretamente no cotidiano social. Como no conhecido caso da Target[1], no qual a equipe de *analytics*, que tinha como intenção identificar as consumidoras grávidas, baseadas em seus perfis de compras, pesquisas e outra informações nesse sentido, acabou por desenvolver um modelo estatístico que previa com bastante acurácia a gravidez, detectando antes mesmo do que própria mãe. Conforme assevera o próprio Duhigg (2012) ao comentar esse caso, "muitas vezes, as nossas vidas possuem muitas informações para conseguirmos perceber o que está a desencadear um determinado comportamento[2]", mas que não passam tão imperceptíveis por uma máquina.

---

[1] GUIDE INVESTIMENTOS. Big Data: Como a Target descobriu uma gravidez antes da família?. 18 de fevereiro de 2019. Disponível em: https://www.oguiafinanceiro.com.br/textos/big-data-como-a-target-descobriu-uma-gravidez-antes-da-propria-familia/ Acesso em: 18 nov 2022

[2] Tradução Livre de: "*Our lives often contain too much information to figure out what is triggering a particular behavior.*" (Duhigg, 2012)

Não se pretende entrar neste tópico nas questões éticas ou filosóficas dessa realidade, mas se quer tão somente demonstrar que a quantidade de dados que estão sendo produzidas nas relações digitais dos indivíduos são suficientes não apenas para traçar de forma fidedigna o perfil de um usuário, como também produzir evidências relevantes sobre pessoas e situações.

Havendo aqui a exata convergência entre a sociedade da informação e sua influência na jurisdição, especificamente no devido processo legal. Uma vez que, as evidências necessárias para as produções probatórias não têm advindo somente do ambiente físico, mas também e principalmente do ambiente digital. A produção massiva de dados possibilita muitas vezes o mapeamento completo de atividades e comportamento de indivíduos que podem ser cruciais em investigações e no livre convencimento do juiz.

É importante ressaltar que a busca e utilização dessas evidências e provas advindas de investigações no contexto digital tem ocorrido pelo menos há duas décadas e tem sido uma realidade prática (Prado, 2021, p.175). E que apenas tenderá a continuar, mesmo que as normativas ainda não estejam acompanhando essa realidade completamente. Uma vez que o mundo está cada vez mais tecnológico e a vida online tem se tornado cada vez mais importante para a efetiva participação no contexto social, boa parte das evidências vão vir do digital. Considerando o contexto de desenvolvimento tecnológico vivido e a constante inserção da Inteligência Artificial em quase todas as esferas da economia, da sociedade e da cultura, não se pode ignorar a possibilidade de seu uso também na produção probatória.

Ressalta-se também que a produção e a inclusão probatória processual deve acompanhar a realidade tecnológica imposta, uma vez que existe um real direito constitucional à prova e este não pode ser preterido em razão de sua forma eletrônica ou digital. Não é coerente que o processo judicial se agarre firmemente ao uso de provas físicas e ignore a realidade da prova digital, uma vez que a prova é direito fundamental e essencial para a devida administração da justiça.

2.1 Aspectos Constitucionais do Direito à Prova no Brasil

A ocorrência do fenômeno jurídico, que leva ao efetivo reconhecimento de um direito, é composta por um fato ocorrido, que deve ser socialmente valorado como relevante a ponto de ser capaz de gerar algum resultado e a norma relativa à situação que integra o fato e valor em questão, deve trazer o efetivo direcionamento.

Até que se chegue ao resultado que designa o sentido de uma norma, os fatos valorados devem ser provados como reais, para que os litígios postos sejam resolvidos e o direito pleiteado seja garantido. Considerando a submissão processual brasileira ao modelo acusatório, tem-se como base a 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.

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) argumenta que o "processo penal e a prova nele admitida integram o que se poderia chamar de modos de construção do convencimento do julgador".

Então, no processo, os fatos que causaram a lide são invocados, com a finalidade de justificar, perante o juiz, a pretensão de um dos autores e a resistência de outro. Do exame dos fatos, o juiz virá com a solução (Theodoro Junior, 2018, p.876). Entretanto, não há como apenas alegar fatos, se eles não forem comprovadamente verdadeiros, não servirão em nada para o processo, uma vez que a decisão final será baseada neles. Assim, a prova vem como um instrumento processual que tem como objetivo atestar a veracidade dos fatos mencionados.

Sobre isso, Humberto Theodoro (2018, p.876) traz uma oportuna citação de Monteiro (1912, p.93) quando diz que a sentença, para que efetivamente declare o direito, de forma que os direitos postulados sejam efetivamente garantidos juridicamente, é preciso que antes de tudo o juiz tenha atestado a verdade do fato alegado. Em seu sentido objetivo, então a prova é o meio hábil para demonstrar a existência de um fato (Theodoro Junior, 2018, p.876). Além de ser o meio pelo qual se forma a convicção do juiz em relação ao fato proposto (Thamay; Tamer, 2022, p.28).

Essa perspectiva também coaduna com a explicação trazida por Távora e Alencar (2019, p. 627) quando dizem que a utilização probatória contribui para a demonstração da verdade dos fatos, sendo prova "tudo aquilo que contribui para a formação do convencimento do magistrado", sendo esta intrinsecamente a finalidade e objetivo do uso da prova. Que é também a perspectiva trazida por Roxin (2003, p.185): "*probar significa convercer al juez sobre la certeza de la existencia de un hecho*".

Ademais, Maier (2011, p.81), em sua definição de prova, explica que se trata de tudo que, no âmbito do processo penal e das regras propostas, produz conhecimento certo ou provável sobre a hipótese contida no processo:

> Intuitivamente resulta sencillo definir la prueba por referencia al conocimiento, como todo aquello que, en el marco de un procedimiento penal y de sus reglas, produce en quien interviene en él un conocimiento cierto o probable acerca de la hipótesis contenido del procedin1iento, la in1putación a una persona de un hecho punible (Maier, 2011, p.81).

Assim, tudo que está dentro da permissão normativa e serve para provar o fato alegado e é suficiente para convencer o juiz, pode ser entendido como prova. Levando em consideração o objeto de pesquisa deste trabalho, pode-se ponderar que os meios probatórios, assim como as normativas, devem acompanhar a realidade social e as mudanças ocorridas. É possível que as normativas processuais não contemplem completamente todas as nuances sociais nesse sentido, mas deve haver mecanismos suficientes para que as provas, a despeito de suas características, se efetivamente lícitas[3], tenham possibilidade de serem juntadas ao processo. Não há coerência, por exemplo, que, em uma sociedade com significativos avanços tecnológicos, não sejam aceitas provas obtidas de meios eletrônicos, sendo apenas acolhidos documentos físicos.

A relevância probatória fica ainda mais evidente quando sua ausência gera interferência direta nas garantias fundamentais de um indivíduo, não apenas refletindo a impossibilidade de se conseguir um direito mediante a comprovação do que se alega, como também o ruído direto na concretização de um trâmite processual digno, que é previsto constitucionalmente.

Dessa forma, é possível compreender que para além de se dar andamento natural à solução de uma lide, provando os fatos postos, a prova também é um importante mecanismo de garantia de direitos fundamentais, sendo de grande relevância na condução processual de uma sociedade de estado de direito democrático.

Segundo Afonso da Silva (2015, p. 180), os direitos fundamentais são princípios que, através de disposições normativas, resumem a visão e a ideologia política de cada ordenamento, designando as prerrogativas e instituições que entende como suficientes e necessárias para garantir uma vida digna, livre e igual para todas as pessoas, não somente em relação ao estado, mas também no âmbito privado. Marmelstein (2019, p.17) diz também que esses direitos estão

[3] Conforme Artigo 5°, LVI, da Constituição Federal de 1988

atrelados ao desenvolvimento de uma vida digna, na qual estão atribuídas a autonomia da vontade, a integridade física, a não coisificação do ser humano e a garantia do mínimo existencial. Trazendo também a visão de Luño (2004, p.20), tem-se que os direitos fundamentais determinam o significado de poder público, em razão da íntima relação entre o papel desses direitos e a forma como as funções do Estado são exercidas e organizadas. Sendo assim, esses direitos são a principal garantia para os cidadãos de um Estado de Direito em que o sistema jurídico e político está orientado para o respeito e promoção da pessoa humana nas suas mais diversas dimensões.

No que se referem às características desses direitos, para que se configurem como fundamentais, a principal, inclusive sustentada por todos os autores anteriormente mencionados (Afonso da Silva, 2015, p. 180; Marmelstein, 2019, p. 17; Luño, 2004, p.20), é a de terem como fonte primária a Constituição. Somente podem ser considerados direitos fundamentais os valores que o poder constituinte formalmente reconheceu a necessidade de proteção especial (Marmelstein, 2019 p.18), como aqueles encontrados no Título II da Constituição Federal. Vale ressaltar que, em razão dessa característica, os direitos fundamentais têm aplicação imediata. Outras características mencionadas por Afonso da Silva (2015, p. 182-184) são a inalienabilidade, não sendo detentores de conteúdo econômico-patrimonial; a irrenunciabilidade, em que apesar de poderem ser deixados de ser exercidos ou não exercidos, não podem de nenhuma forma serem renunciados; e a Imprescritibilidade, não se verificando requisitos que levem à sua prescrição. Uma última característica mencionada por Marmelstein (2019, p.17), e que se entende relevante mencionar, seria a importância axiológica desses direitos, sendo capazes de fundamentar e legitimar todo o ordenamento jurídico, com força para afetar a interpretação de qualquer norma jurídica.

Adentrando a análise constitucional, especificamente no que se refere ao princípio da inafastabilidade da jurisdição[4], há uma necessidade de atuação positiva do Estado no sentido de solucionar de forma adequada os litígios que culminaram em lesão ou ameaças a direitos. Por meio desse princípio, há a preconização do estado de "dever ser" das coisas que deve ser buscado, como o pleno acesso à jurisdição. A aplicação desse princípio não se justifica somente na necessidade de seguir a letra da lei, submetendo a ela o fato, "[...] mas também pela verificação se os fatos e dispositivos contribuem para esse acesso ou não" (Tamer, 2017, p.118). Assim, o acesso à justiça será consolidado mediante ao equilíbrio entre os instrumentos

[4] Conforme Artigo 5° XXXV, da Constituição Federal de 1988.

processuais e os direitos materiais, os quais "[...] se perfazem em suportes fáticos e esses são demonstrados a partir dos meios probatórios" (Thamay; Tamer, 2022, p.18), sendo adequado que as normas processuais viabilizem a realização das provas e que essa atividade seja coerente com a realidade posta.

O sistema processual brasileiro está ancorado no conceito de devido processo legal[5], que aponta diretamente para sua configuração garantista (Vaz, 2012, p. 39). Dessa forma, o processo deve buscar não apenas o efetivo exercício da jurisdição, mas também a segurança aos indivíduos de que seus direitos serão preservados. Com isso, vale trazer a perspectiva de Vaz:

> Com a evolução de seu conceito, o devido processo legal passou a ser considerado em *duas dimensões: processual e substantiva*. Em seu significado processual, o devido processo legal corresponde à ideia de um "processo estritamente legal em que se dão às partes as oportunidades amplas de alegar e provar". Na acepção substantiva, o devido processo está relacionado à elaboração da lei conforme processo legislativo previamente definido, bem como à razoabilidade e ao senso de justiça de seus dispositivos (Vaz, 2012, p. 40) (grifo do autor).

Ademais, um indivíduo não poder ter seus direitos restringidos sem que antes tenha-se passado por um processo devido, e este só será assim considerado mediante a aplicação dos meios e recursos inerentes à realização dos princípios do contraditório e da ampla defesa[6]. Uma vez que o princípio do contraditório refere-se ao dar ciência às partes de tudo que ocorre no processo e de que elas têm a possibilidade de serem ouvidas sobre qualquer questão levantada no processo, a prova se encaixa como um meio eficaz nesse contexto de exposição dos pontos de cada lado da lide. Em relação à ampla defesa, sendo esta a qualificação do contraditório, a esse princípio a prova se adequa de forma natural, já que se trata da possibilidade de utilização de todos os meios que a lei permita para a realizar uma defesa, de forma a influir no convencimento do juiz.

Conforme aduzem Thamay e Tamer (2022, p.23), os princípios anteriormente mencionados "sem o mecanismo da prova seriam como almas errantes em busca de seus corpos que pudessem lhes dar vida concreta". não haveria efetivo acesso jurisdicional sem que o indivíduo pudesse validar os fatos que colocou em questão. Ademais não haveria processo justo sem que as partes tivessem ciência de que podem usar de diversos meios probatórios para convencer o juiz e que estes serão devidamente apreciados.

---

[5] Conforme Artigo 5°, LIV da Constituição Federal de 1988.
[6] Conforme Artigo 5°, LV da Constituição Federal de 1988.

A única limitação que o direito à prova enfrenta é a impossibilidade do uso de provas ilícitas[7], no qual entra em direto conflito com outros princípios assegurados pela justiça. Não há que se fundamentar um processo, sem parâmetros claros na produção probatória, uma vez que daria margem significativa arbitrariedade e iria totalmente de encontro ao bom desenvolvimento do estado democrático de direito. Essa vedação não apenas direciona os limites de produção de prova, como também confirma a natureza constitucional do direito a prova (Thamay; Tamer, 2022, p.26).

Conforme constatam Thamay e Tamer (2022), o direito à prova se enquadra seguramente no conceito de direito fundamental, uma vez possui eficácia absoluta e a aplicabilidade imediata, na qual apesar da existência de diversas normativas delineando a utilização de provas em um determinado processo, esse direito será gozado mesmo que esteja fora dos "limites" imposto, uma vez que há respaldo constitucional. Por essa razão, o direito à prova torna-se um dos direcionamentos base do Estado de Direito, dando sustentação normativa aos valores da comunidade. Não há como existir um Estado Democrático com privação desse direito aos cidadãos; não há efetiva garantia da dignidade humana se qualquer norma ou dispositivo normativo infralegal venha a impedir a realização desse direito no processo. O que configura a inalienabilidade, a irrenunciabilidade e a irrevogabilidade do direito à prova.

Sendo uma prerrogativa constitucional, o direito à prova não se refere apenas as relações do cidadão com o Estado, mas também possui eficácia horizontal, irradiando para as relações privadas. Mesmo frente a questões processuais do direito privado, a prova deve se fazer presente, não podendo ser retirada. Além de ser um direito de observância universal, no qual todas as pessoas jurídicas são titulares, não se podendo fazer acepção de quem poderá usufruir desse direito.

Assim, a prova entra como um instrumento garantidor da dignidade humana, sendo crucial para concretização dos direitos de um cidadão participante de uma sociedade democrática e que pode usufruir de suas liberdades e garantias. Privar um indivíduo do direito à prova não se trata somente de proceder contra o direito positivado, mas contra o mínimo existencial de um humano.

Do exposto, além de evidências relativas à natureza de direito fundamental à prova, há que se falar da "brecha" à aceitação da inclusão da prova digital no processo brasileiro. Uma

[7] Conforme Artigo 5°, LVI, da Constituição Federal de 1988.

vez que a jurisdição não pode se eximir de aceitar a apreciação de uma prova somente em razão da não previsão direta em seu texto normativo. Ademais, como está enquadrada como direito fundamental constitucional, não há óbices ao uso da prova em razão de uma possível atipicidade, se é capaz de provar o fato de forma lícita e devida.

Ocorre que antes da prova em si, há existência das evidências, que são como vestígios que podem contribuir ou não para formação de uma prova. A presença intrínseca da tecnologia prova essa realidade ao permitir que a todo momento os indivíduos estejam produzindo algum tipo de evidência em razão de suas interações com o digital, como geolocalização em um determinado dia, hora de acesso aos dispositivos, pesquisas realizadas em seu navegador, preferencias direcionadas em sites visitados etc. Todas essas informações são evidências, que por si só nem sempre são capazes de atestar fatos, mas se unidas a outras informações, preservando a forma processual estabelecida, podem gerar uma prova válida que será integrada ao processo.

2.2 Evidências e Provas

Segundo Casey (2011, p.3), na era moderna é difícil imaginar um crime que não tenha nenhum tipo de dimensão ou influência digital. Uma vez que apesar de muitos deles ocorrerem no mundo físico, boa parte dos vestígios e pistas podem ser encontrados nos meios digitais. Apesar de ninguém poder ser morto via rede de computadores, pessoas tem cometido suicídio depois de serem vítimas de *cyberbullying* (Casey, 2011, p.4) ou mesmo assédios e conversas virtuais que culminaram em crimes de abuso, dentre outros diversos exemplos.

Trazendo de volta a perspectiva anterior sobre sociedade da informação, grande número de dados produzidos e uso contínuo da tecnologia no dia a dia dos indivíduos, há que se lembrar que o aspecto "positivo" de toda essa inserção da tecnologia no cotidiano social é a grande quantidade de evidências e provas digitais que podem ser utilizadas no processo judicial para deter e processar os infratores, sendo por vezes inclusive a única pista em uma investigação (Casey, 2011, p.5). Isso porque mesmo que os dados digitais não forneçam uma ligação entre um crime e a sua vítima ou um crime e o seu autor, podem ser úteis numa investigação. Já que "o homem por natureza, é produtor de informações (...)" (Barreto, Wendt, 2020, p.30), as evidências digitais podem revelar a forma como um crime foi cometido, fornecer pistas de investigação, refutar ou apoiar declarações de testemunhas e identificar prováveis suspeitos (Casey, 2011, p.6).

Evidências seriam como dados avulsos, de situações rotineiras, mas que se unificados, podem gerar uma informação útil e esta pode ser relevante em investigações. Por exemplo, o caso de Robert Durall[8], que foi condenado pelo assassinato de sua mulher, e dentre as evidências que foram basilares para a solução do caso estão as pesquisas feitas na internet com as seguintes palavras “"sufocação", "homicídio", "cônjuge + matar" e "sono + comprimidos + morte"”, logo antes da morte de Carolyn. Assim, é possível perceber que a pesquisa em si não levaria necessariamente a concluir que seriam referentes a um assassinato. Entretanto, quando juntadas a informações como quem as fez, as cartas da esposa relativas à insatisfação com seu marido e os abusos sofridos e seu desaparecimento, trazem uma perspectiva diferente.

Trazendo a definição da Standard Working Group on Digital Evidence (SWGDE), adicionada em seu glossário, tem-se que evidências digitais são “informações de valor probatório que são armazenadas ou transmitidas em formato binário”[9]. Ademais, de acordo com Association of Chief Police Officers, na versão 4.0 do “*Good Practice Guide for Computer-Based Electronic Evidence*” (Wilkinson, Haagman, 2010, p.6)[10], são informações e dados de valor investigativo que são armazenados ou transmitidos por um computador. Nessa perspectiva, Carrier (2006) também diz que são dados digitais que apoiam ou refutam uma hipótese sobre eventos digitais ou o estado dos dados digitais. Coaduna com essas definições também o conceito dado por Peck (2021, p. 96), quando explica que a evidência digital “é toda a informação ou assunto criada e sujeita, ou não, a intervenção humana, que possa ser extraída de um computador ou de qualquer outro dispositivo eletrônico”.

Dessa forma, as evidências são como dados soltos com valor probatório, que podem ser fundamentais no estabelecimento de ligações entre fatos e informações em um determinado caso. Especificamente, evidências digitais, são esses mesmos dados, mas quando obtidos digitalmente. Seria como uma informação crua, não necessariamente ligada a um fato em si,

---

[8] Disponível em: https://archive.seattletimes.com/archive/?date=20000508&slug=4019710. Acesso em: 18 out 2023

[9] “*Information of probative value that is stored or transmitted in binary form*.” Scientific Working Group on Digital Evidence. ASCLD Glossary Definitions: Version 3.0, 2016. Disponível em: https://www.swgde.org/glossary. Acesso em: 23 out. 2023

[10] “*Computer-based electronic evidence is information and data of investigative value that is stored on or transmitted by a computer*.” Association of Chief Police Officers. Good Practice Guide for Computer based Electronic Evidence: Version 4.0, 2005. Disponível em: https://www.datainvestigations.co.uk/files/ACPO%20Guidelines%20Computer%20Evidence%20v4.pdf. Acesso em: 25 out. 2023

mas que, quando unida a outras informações, podem oferecer pistas relevantes. Entretanto, para que essas evidências sejam utilizadas, elas devem ser inseridas no processo como provas válidas.

Levando em consideração o caso anterior, as pesquisas realizadas por Durall fornecem pistas inegavelmente relevantes, entretanto não podem ser colocadas no processo de qualquer forma. É necessário que seja atestado a veracidade da pesquisa, que realmente foi feita em um dispositivo operado por ele, a hora que foi realizada, o que foi lido etc. E isso só pode ser feito mediante um perito, que seria capaz de atestar inequivocamente todos esses pontos, produzindo a prova a ser juntada processualmente.

A prova então é o meio utilizado para atestar os fatos alegados em uma lide, de forma a convencer o juiz e ajudá-lo a formar sua posição e garantir (ou não) os direitos postulados pelas partes. Theodoro Júnior (2018, p.878) diz que toda prova tem um objeto, uma finalidade, um destinatário e deve ser obtida através de meios e métodos previamente estabelecidos. Assim, como objeto da prova temos os fatos que geraram algum desdobramento jurídico, a finalidade seria o convencimento em relação à veracidade desses fatos e o destinatário é o juiz, uma vez que precisa ser convencido.

No que se refere especificamente à obtenção das provas, 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. (Minto, 2021, p. 27). É o que se utiliza para comprovar o fato que é posto em questão (Theodoro Junior, 2018, 878). É a pessoa ou a coisa da qual a prova emana. (Távora; Alencar, 2019, p.629). Então como exemplos de fonte, poderíamos identificar uma pessoa, um cadáver, um escrito, a internet, plataformas digitais, algoritmos etc.

O “meio de prova” 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, p. 27). São os instrumentos processuais disponíveis para a produção da prova (Távora; Alencar, 2019, p.629). Segundo Lopes Júnior. (2021, p.175), é o recurso utilizado para oferecer ao juiz condições de formação da história do fato, os quais os resultados influenciarão diretamente na decisão. Como exemplo cita-se a prova testemunhal, documentos e perícias. Há diferença entre meio de prova e meio de obtenção de prova, pois este é referente os instrumentos que permitem se chegar à prova (Lopes Júnior, 2021, p.175), sendo em regra extraprocessuais (Távora; Alencar, 2019, p.629).

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, p. 27). É o que se extrai da prova em relação ao fato, pode ser a comprovação ou a negação de tudo que as partes alegaram. Assim, prova refere-se aos instrumentos aptos à produção, explicação e comprovação.

Do exposto, é possível compreender que as evidências encontradas somente serão levadas ao processo uma vez que forem consideradas como provas aptas e válidas. Mesmo que a informação seja diretamente relevante para o processo, não irá sem que seja levado em consideração todo o processo previsto para que seja compreendida como prova. É exatamente o que expõe Neres (2021, p. 346) ao explicar o que se segue:

> Em resumo, podemos entender o vestígio digital como um dado digital que possa ter relação com o fato investigado. Já a evidência digital pode ser considerada um vestígio digital analisado e comprovadamente relacionado ao caso investigado. **A prova digital, por sua vez, é a evidência digital formalizada no âmbito processual**. (grifos do autor).

Nesse sentido, há que se falar também da validade das provas e a coerência formal e material que devem ter. Tanto o Código de Processo Civil, quanto o Código de Processo Penal, trazem previsões muito claras sobre a necessidade de as provas serem obtidas de fontes lícitas e moralmente legítimas, fora disso serão inadmissíveis. Assim, se uma prova violar disposições de direito material ou princípios constitucionais, ela será ilícita. Sendo assim, a prova deve ser sumariamente excluída do processo, não podendo ser de forma alguma utilizada para fundamentação da decisão do juiz. Se, por outro lado, acabar por violar as normativas processuais e os ritos corretos para sua obtenção, será ilegítima. E, nesse caso, deverá ser reconhecido o tipo de nulidade, se absoluta, relativa ou mera irregularidade, a depender do caso, pode ser ainda utilizada no processo (Távora; Alencar, 2019, p.643).

Vale ainda ressaltar que dentro da perspectiva de provas válidas, as provas podem ser típicas ou atípicas, podendo ter dispostas na lei a forma procedimental para que sejam constituídas ou não (Távora; Alencar 2019, p.639). Laronga (2002, p.6-7) 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, p. 8) explicam:

> [...] as caracterizações da tipicidade ou da atipicidade da prova decorrerão de cinco situações possíveis: a) o meio de obtenção ou de produção de prova está previsto e é regulado mediante procedimento próprio; b) o meio de obtenção ou de produção de prova está previsto, não está regulado, mas há remissão ao procedimento a ser seguido; c) o meio de obtenção ou de produção de prova está previsto, não está regulado e não

> há remissão a nenhum procedimento a ser seguido; d) o meio de obtenção ou de produção de prova é apenas referido nominalmente, sem qualquer regulamentação ou remissão ao procedimento a ser seguido; e) o meio de obtenção ou de produção de prova não é sequer referido. Serão típicos os meios de obtenção ou de produção de prova quando ocorrentes as situações descritas nas letras a), b), e atípicos quando configuradas as situações das letras c), d) e e) (Fernandes; Almeida; Moraes, 2011, p. 8).

É possível compreender que há possibilidades de aceite de uma prova mesmo que ela não esteja prevista ou que não tenha procedimento estabelecido. É essa inclusive a disposição direta do Artigo 396 do Código de Processo Civil. Ademais, no Artigo 13 da Lei 11.419 de 19 de dezembro de 2006, há disposição deque o "magistrado poderá determinar que sejam realizados por meio eletrônico a exibição e o envio de dados e de documentos necessários à instrução do processo", uma autorização legal para que o juiz possa determinar a produção de provas digitais típicas ou atípicas (Barzotto, 2022, p. 101). Lopes Junior (2011) ainda explica que, pode-se aceitar excepcionalmente provas atípicas, desde que dentro dos limites constitucionais e processuais, esse seria o caso específico das Provas Digitais que será abordado futuramente. Assim, 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 à 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. Vale trazer a análise feita por Thamay e Tamer (2022):, p. 19):

> O acesso à função jurisdicional adequado 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 a realidade (Thamay; Tamer, 2022, p. 19).

Portanto, se a prova estiver apta a demonstrar a veracidade de um fato e estiver dentro dos parâmetros de legalidade não há razão para 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 dever ser entendida como excepcional.

De todo o exposto, não é prudente confundir evidências com provas. Apesar de aquelas estarem contidas dentro destas, possuem diferenças e assim precisam ser compreendidas. Entretanto, não haverá prova, se antes não existirem evidências disponíveis, com potencial probatório, para que sejam formalmente analisadas e integradas ao processo. As evidências, então, estão dispersas no mundo físico e no digital, cabe a melhor coleta e preservação possível destas, para que consigam atingir o devido valor probatório e então possam ser consideradas como provas.

3 TEORIA GERAL DA PROVA DIGITAL

A realidade das provas digitais é inevitável, uma vez que, conforme explica Meireles (2023), a sociedade encontra-se inserida na era digital, na qual as tecnologias têm afetado todas as realidades, particularmente a vida social e humana, de forma que há uma dependência real da internet, de aplicativos, aparelhos informáticos, sem os quais já não há mais como viver. Veja-se o exemplo do próprio computador: não há mais quem queria escrever sua dissertação, tese ou artigo à mão ou que dependa completamente de uma máquina de escrever. Quer-se hoje o computador, o notebook, com um aplicativo da Microsoft que permita uma escrita corrida, com fácil edição, possibilidade de correção ortográfica etc.

Uma vez que a Era Digital tem produzido efeitos em todos os ramos da vida quotidiana, não era improvável que tivesse também influencia na justiça, nos atos processuais e na condução da produção probatória. Entretanto, nesse campo específico, ainda há uma série de questões controversas sobre a validade inclusão definitiva no processo, a forma correta de coleta, os princípios norteadores de seu uso, bem como os limites que devem ser considerados para que os direitos fundamentais sejam preservados.

Em razão da tecnologia, do advento da internet e a dispersão dos dispositivos móveis, vive-se numa sociedade de constante vigilância, em que realmente há acesso continuo a todo tipo de evidência e informação. Quase todas as ações humanas têm produzido dados, que estão sendo de alguma forma armazenados e posteriormente utilizados para finalidades diversas. Negar que o direito deve abranger essa realidade é incoerente, uma vez que se caminha para uma completa digitalização das atividades.

A utilização de provas e evidências digitais já é então uma realidade, pode não estar completamente normatizada, mas a prática já ocorre há tempos, mediante o uso de conversas em redes sociais, e-mail, gravações realizadas por assistentes digitais, dados de geolocalização

armazenados em dispositivos móveis e relógios inteligentes e até mesmo dados constantes em bancos de dados e aplicativos. Coaduna-se com esse pensamento Meireles (2023, p. 93) ao explicar que a realidade da justiça hoje não se trata apenas dos elementos encontrados no processo tradicional (com provas com faturas, contratos e outros documentos no sentido tradicional da palavra), mas há também a inclusão da realidade em rede, na rapidez de conexão e relacionamentos virtuais, de realização de contratos, de dispersão de informações e a própria desmaterialização da comunidade.

Vale expor as exatas palavras de Meireles (2023, p. 93) ao dizer que "[a] justiça está influenciada pela sociedade digital não só no seu acesso, como na sua tramitação, mas sobretudo, como o próprio caminho para desburocratização e desmaterialização". A inclusão do digital na justiça gera não apenas uma adequação à realidade de uma era, mas também a celeridade nos processos.

A tendência é que essa realidade se perpetue, não apenas em razão da contínua produção de dados pelos indivíduos dia após dia, mas também da diversidade de formas que são constantemente desenvolvidas para coletar esses dados. Por exemplo, antes, a forma de obter imagens diversas de usuários (Biometria) para treinar Inteligência Artificial era pela coleta de fotos dos usuários de redes sociais que faziam o *upload* em seus perfis de redes sociais. Atualmente, diversos aplicativos que prometem a entrega de imagens prospectivas das pessoas têm ganhado força e bastante utilização, e o retorno obtido aos desenvolvedores é uma porção significativa de fotos, dos indivíduos que querem esse serviço, que serão usadas em testes em IA

Levando ainda em consideração este exemplo, pode-se entrar numa discussão em torno da proteção de dados dos indivíduos, consentimento consciente e desvio de finalidade da utilização dos dados. Em caso de um suposto processo nesse sentido, as provas deveriam ser advindas do aplicativo, dos softwares que receberam os dados coletados etc. Diante dessa situação hipotética, as seguintes perguntas são levantadas: "Como as provas nesse caso serão obtidas?"; "Tendo sido obtidas, como serão incorporadas ao processo? Serão entendidas como válidas?"; "Serão legalmente aceitas no processo?".

Essas perguntas são as exatas questões pendentes no que se refere às provas digitais, que apesar de serem uma realidade no que se refere ao processo, ainda não têm o seu uso totalmente consolidado normativamente falando. Dessa forma, há que se entender o que são as

provas digitais, quais suas características e particularidades, o que é necessário ser levado em consideração em sua cadeia de custódia para serem acopladas ao processo e seus elementos de validade.

3.1 Prova Digital: conceito e características

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" (Casey, 2011, p.17).

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*), trazem a seguinte definição: "Informações de valor probatório armazenadas ou transmitidas em formato digital[11]" (SWGDE, IOCE, 2000).

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". Já Thamay e Tamer (2022, p.32) entendem que prova digital poderá ter duas acepções:

> Uma primeira, segundo a qual a prova digital pode ser entendida como a demonstração de um fato ocorrido nos meios digitais, isto é um fato que tenha como suporte a utilização de um meio digital. E, uma segunda, em que, embora o fato em si não tenha ocorrido em meio digital, a demonstração de sua ocorrência pode se dar por meios digitais (Thamay; Tamer, p.32).

Vaz (2012, p.63) 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." Ainda, Meireles (2023, p. 100-101) diz que "prova digital é toda informação, independente do suporte em que se apresente, que tenha sido criada ou obtida através de dispositivos integrados em redes digitais". Dessa forma, provas digitais

[11] Scientific Working Group on Digital Evidence (SWGDE), International Organization on Digital Evidence (IOCE). Digital Evidence: Standards and Principles, Forensic Science Communications, V 2, N 2, April 2000. Disponível em: https://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm. Acesso em: 12 de fev. 2023

são meios de demonstração de uma situação ocorrida dentro do contexto digital, ou cujos dados armazenados digitalmente sejam suficientes para explicar um fato.

É importante pontuar que 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), p. 63). Além do que não deve ser confundida com prova eletrônica, que, segundo Casey (2011, p. 17), seria o gênero em comporta a espécie que é a prova digital.

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 elas que individualizam como categoria específica de fonte de prova (Vaz, 2012, p. 63). O que coaduna com a análise feita por Minto (2021, p. 16) quando diz que "[n]esse contexto, parece ganhar cada vez mais relevância a necessidade de um regramento específico do instituto, especialmente diante do reconhecimento de suas características próprias [...]".

É possível perceber que há entendimento pacífico de pelo menos três características das provas digitais, são elas a imaterialidade, a volatilidade ou fragilidade e alto potencial dispersão. A imaterialidade é referente a natureza impalpável dos dados que se referem à prova digital (Vaz, 2012, p. 68) e que existem independentemente de qualquer suporte físico (Minto, 2021, p. 35). Diferentemente da produção de prova tradicional, na produção da prova digital não se irá buscar identificar o local onde o crime foi cometido, uma vez sendo bastante um dispositivo (computador ou celular) ligado à internet. Assim, o "lugar" do crime pode ser qualquer região do mundo, como lojas, cafés, ou pontos de acesso a redes públicas (Almeida, 2015, p, 32). Além do que, fácil mobilidade dos aparelhos também permite uma rápida dispersão geográfica do infrator, tornando-o imprevisível e volátil, entrando na segunda característica da prova digital.

A volatilidade ou fragilidade diz respeito a facilidade de alteração ou desaparecimento a que aquela evidência está submetida, ou seja, não há fixação material da prova. Assim a prova pode desaparecer em razão de determinados eventos, sendo intencionais ou não (Minto, 2021, p. 35-36). Há uma facilidade de se apagar qualquer tipo de indício probatório com ações simples, como a limpeza do histórico de navegação, a exclusão de um arquivo ou a adulteração de um

documento por simples edição do conteúdo. Mas há também outros meios, como alterações de permissões, uso de VPNs e até mesmo a criptografia de arquivos.

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). Um crime cibernético pode interferir na vida de um indivíduo que mora na América, mas o infrator pode realizar sua atividade da Oceania, por exemplo. Ou então um mesmo arquivo pode ter suas partes armazenadas em uma base de dados cujo operador é europeu, o outro é africano e a jurisdição que busca acesso é norte americana.

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 melhor regulados e especificados.

Antes que se prossiga para a efetiva análise sobre a obtenção das provas digitais, é coerente analisar brevemente sua natureza jurídica, no que se refere a sua tipicidade ou atipicidade. Embora, até o presente momento neste trabalho tenhamos direcionado o entendimento para a atipicidade da prova digital, em razão de suas características intrínsecas e particularidades, há uma tendência doutrinária no que diz respeito a natureza jurídica da prova digital, colocando-a como uma prova documental (Silveira, 2015, p. 229).

Sendo assim classificada, a prova digital, poderia ser facilmente enquadrada em alguns artigos esparsos da jurisdição brasileira, como o artigo 225 do Código Civil, sobre prova documental, que dispõe que diversos tipos de reproduções, dentre elas “quaisquer outras reproduções mecânicas ou eletrônicas”, são capazes de fazer prova plena dos fatos e das coisas a que se referem, desde que não sejam impugnados no que se refere a exatidão. Ou seja, a prova apresentada deve necessariamente corresponder ao documento original (Capanema, 2024, p. 204). Ou poderiam também ser enquadrados nos artigos 439 a 441 do Código de Processo Civil, que são disposições diretas sobre documentos eletrônicos. No artigo 439 há dois requisitos principais indicados para que a prova seja considerada no processo, que são: (i) a conversão à forma impressa, e (ii) a verificação da autenticidade. No artigo 440 há determinação de que o juiz deverá apreciar o valor probante dos documentos eletrônicos não convertidos. E, no artigo

441 declara que a admissão dos documentos eletrônicos se dará mediante a observância na produção e conservação da legislação específica, que parece ser a Lei do Processo Eletrônico ou a Medida Provisória 2.200-2/2001 (Capanema, 2024, p. 206), mas que não tratam especificamente da prova digital.

Analisando os dois dispositivos mencionados, é possível compreender que até poderiam produzir efeitos satisfatórios no que se refere ao processo civil, ocorre que as características documentais nem sempre irão bater com as características da prova digital em si. Por exemplo, no processo penal, já não seria viável, uma vez que há uma restrita definição no artigo 232 do conceito de documento, que são quaisquer escritos, instrumentos ou papéis, públicos ou particulares, o que não abarca a prova digital, que nem sempre virá de forma escrita, nem mesmo em papel, muitas vezes será apenas um conjunto binário de números, ou um áudio e nem sempre sua autenticidade poderá ser comprovada por assinaturas digitais ou chaves públicas.

Dessa forma, uma vez que aqui se trata da aplicação geral da prova digital, não é coerente sustentar sua natureza jurídica como típica já que não seria aplicável a qualquer contexto processual, que é a finalidade de análise dessa pesquisa. Sendo então razoável considerar a prova digital como prova atípica, mas que possui a mesma capacidade de convencimento de qualquer outra prova lícita típica, já que a "despeito de não estar expressamente prevista na legislação processual penal, pode ser admitida em função do princípio da liberdade da prova" (Silveira, 2015, p. 230).

Ademais, não há nenhum direcionamento normativo específico sobre a admissibilidade e forma de produção desse tipo probatório, conforme Marinoni e Arenhart (2019, p. 660) explicam, há uma carência significativa de normativas que tratem da força probante dos documentos produzidos digitalmente, uma vez que é difícil ser comprovada a autenticidade da informação digitalmente transmitida, conforme visto nos dispositivos mencionados anteriormente, no fim sempre haverá a necessidade de comprovação de autenticidade da prova, o que nem sempre poderá ser feito pelos mesmo meios e métodos previstos para a prova documental. Portanto, nesse trabalho, adota-se a compreensão de que a prova digital é um meio atípico de prova.

3.2 Meios de obtenção da prova digital

A coleta de provas digitais é evidentemente diferente da coleta de provas tradicionais ou físicas. A distinção é tão significativa que as regras para as antigas investigações muitas vezes não fazem mais sentido para as novas (Kerr, 2005, p. 280). Não é coerente buscar recolher documentos físicos ou coletar depoimento de testemunhas oculares, por exemplo, já que frequentemente os crimes ocorrem dentro do contexto digital e as regras e normativas antigas já não se aplicam a esse contexto em diversos aspectos.

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. O Brasil, por meio do Decreto Legislativo n° 255 de 2021, aprovou o texto da Convenção, aderindo ao regramento.

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[12]. No que se refere especificamente à produção e obtenção de provas, a Convenção de Budapeste aponta quatro meios principais. (i) Preservação expedita de dados armazenados, (ii) Ordem de exibição, (iii) Busca e apreensão de dados de computador; e (iv) Obtenção de dados de computador em tempo real.

O primeiro, que se encontra nos artigos 16 e 17, trata da conservação expedita de dados informáticos armazenados. Seria exatamente a possibilidade que as autoridades competentes têm de ordenar a preservação de dados informáticos específicos, como forma de conservar para que futuramente sejam utilizados como prova (Minto, 2021, p. 37-38). A importância desse meio se mostra frente à 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 da ordem de produção, ou injunção. Que diz respeito a 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,

[12] Disponível em: https://opiceblum.com.br/convencao-de-budapeste-e-promulgada-sob-a-forma-do-decreto-legislativo-no-37/. Acesso em 10 de fevereiro de 2023.

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 as buscar de sistemas ou suportes informáticos (Minto, 2021, p. 38). Diferentemente do meio anterior essa busca 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 se busca obter informações no meio de uma transmissão de dados e não entre dados já armazenados previamente (Minto, 2021, p. 39). Essa divisão coaduna com a posição Kerr (2005, p. 285):

> 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 (Kerr, 2005, p. 285) (grifos do autor).

Do exposto é possível compreender que 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. Submete-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.

3.3 Obtenção da Prova Digital no Contexto Processual Brasileiro

Apesar da submissão à Convenção de Budapeste, atualmente a legislação brasileira não possui uma normativa específica que trate de provas digitais. Vale mencionar que há um Projeto de Lei (4.939/2020), ainda em tramitação, que visa o estabelecimento de "princípios e diretrizes na aplicabilidade do Direito da Tecnologia da Informação, bem como normas de obtenção e admissibilidade de provas digitais na investigação e no processo, definindo crimes e penas". Apesar, disso, não há como efetivamente analisar o texto proposto, uma vez que não

pode ser aplicado efetivamente à realidade brasileira, já que ainda não foi aprovado. Entretanto, há alguns diplomas legais que fazem referência a obtenção de provas digitais, os quais são relevantes para essa análise.

O primeiro desses é a Lei 9.296/96 (Lei de Interceptação de Comunicações Telefônicas, Interceptações Telemáticas e Captação Ambiental), que veio como regulamentador do Artigo 5°, XII da Constituição, e cujo objetivo é possibilitar o acesso a comunicações telemáticas para acessar evidências referentes a algum delito. Logo em seu primeiro artigo há o direcionamento da aplicabilidade da lei em sistemas de informática e telemática. Analisando esses acessos, é possível enquadrá-los exatamente no que prevê o título 5, da Seção 2, da Convenção de Budapeste como "obtenção de dados de computador em tempo real", no qual haverá a entrada no meio de uma comunicação e o acesso a informações de um ambiente específico.

Vale ressaltar, que a própria lei traz a excepcionalidade do uso desses mecanismos. Sujeitando a utilização a alguns requisitos, como a prova não poder ser feita por outro meio indícios razoáveis de autoria e participação em infração penal. Assim, não se poderá aplicar com facilidade o que traz a Lei de Interceptação Telefônica, já que uma vez obtidas as provas fora dos requisitos propostos, haverá razões suficientes para não ser entranhada ao processo e de nada adiantou o uso dos dispositivos e serviços eletrônicos.

O segundo diploma legal que podemos citar é o Marco Civil da Internet, a Lei 12.965/14, cujo objetivo é estabelecer princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Em alguns artigos específicos têm-se alguns direcionamentos relacionados a produção de provas digitais, como no Artigo 10 e 13, os quais tratam da guarda de informações e a possibilidade de disponibilização dessas informações mediante ordem judicial. Há também o artigo 22 que trata especificamente da possibilidade das partes interessadas requererem ao juiz ordem judicial para fornecimento de registros de conexão ou de registros de acesso a aplicações de internet, e assim formarem o conjunto probatório do processo.

Trazendo novamente a análise anterior feita em relação a Convenção de Budapeste, esses artigos se assemelham aos Títulos 2 e 3 que preveem respectivamente o armazenamento dos dados e uma possível ordem de exibição desses dados. Os outros diplomas legais que trazemos são a Lei 8.069/90 (Estatuto da Criança e do Adolescente - ECA) e a Lei 12.850 (Lei das Organizações Criminosas). Apesar de serem normativas com objetivos bem distintos, no

que se refere à prova digital, tratam de Infiltração Virtual. No ECA, esse mecanismo foi introduzido através da Lei 13.441, em 2017, estabelecendo que seria aplicável aos crimes de pedofilia, previsto nos artigos 240 a 214-D da respectiva lei; nos crimes de estupro de vulnerável, corrupção de menores, satisfação de lascívia mediante presença de criança ou adolescente e favorecimento de prostituição ou de outra forma de exploração sexual de criança ou adolescente ou vulnerável, previstos nos artigos 217-A a 218-B do Código de Processo Penal; e especificamente no crime de invasão de dispositivo informático, previsto no artigo 154-A também do CP.

Nessa ocasião estão estabelecidos três requisitos para que a prova seja produzida: (i) autorização judicial, que estabelecerá os limite da infiltração, e tendo sido obrigatoriamente ouvido o Ministério Público; (ii) requerimento do Ministério Público ou representação do delegado de polícia, contendo todas as informações sobre a infiltração, como a necessidade, alcance das tarefas do policiais, os nomes do investigados e os dados de conexão para identificação das pessoas, e (iii) realização num prazo de 90 (noventa) dias, podendo ser estendido, mas não podendo ultrapassar 720 (setecentos e vinte) dias, além de ser demonstrada a efetiva necessidade. Além disso, o parágrafo 3° do artigo 190-A, reitera a excepcionalidade da prova, uma vez que só poderá ser assim obtida se não houver outros meios.

Na Lei das Organizações Criminosas, a infiltração virtual foi incluída pelo Pacote Anticrime, Lei 13.964, nos artigos 10-A a 10-D. Nesse caso está voltada a aplicação dos crimes previstos nessa normativa. Assim como a infiltração virtual prevista no ECA, que está submetida a alguns requisitos: (i) a autorização judicial, devendo ser representada pelo delegado de polícia ou requerida pelo Ministério Público; (ii) a demonstração da necessidade e o alcance das tarefas dos policiais; e (iii) a indicação dos nomes ou apelidos das pessoas investigadas os dados de conexão ou cadastrais que permitam a identificação dessas pessoas. Nesse caso, a infiltração poderá durar até seis meses, podendo ser renovada, desde que também o total não exceda 720 (setecentos e vinte) dias. E assim, como no ECA, o parágrafo 3°, do artigo 10-A, também indica a excepcionalidade da obtenção dessas provas.

Da exposição desses diplomas legais, há três importantes considerações a serem feitas. A primeira em direção a percepção do caráter excepcional que é dado a esse tipo de prova, sendo subsidiária, só podendo ocorrer em razão da inexistência de quaisquer outros meios. A segunda é em razão da necessidade de submissão a diversos requisitos e processos para que seja habilitada a efetiva produção da prova, não havendo possibilidades mais simples para seja

melhor direcionada ou que seja obtida com mais celeridade. E a terceira seria o grande direcionamento normativo no campo na criminologia e do processo penal.

Entretanto, apesar do exposto, sabe-se que as provas digitais têm sido produzidas e frequentemente adicionadas ao processo, e esse processo merece atenção, uma vez que a inclusão de uma prova legalmente inválida pode gerar sérios riscos aos direitos individuais das partes envolvidas. Mesmo com a possibilidade de obtenção válida, a prova digital deve passar por uma análise mais criteriosa antes de efetivamente estar efetivamente entranhada no processo, para isso é necessário avaliar a Cadeia de Custódia da obtenção dessa prova.

3.4 Cadeia de Custódia da Prova Digital

A obtenção da informação realmente tem múltiplas formas, entretanto, quando se trata de incorporação a um procedimento judicial, a análise do processo de obtenção importa para que se possa dar efetiva validade e confiabilidade a prova. Nesse ponto específico já é incorporada uma certa dificuldade, uma vez que essa coleta deve levar em consideração as características anteriormente citadas (imaterialidade, a volatilidade e alto potencial de dispersão) e todo o processo deve ser minuciosamente coerente para que seja mantida a fiabilidade da prova que se que incorporar ao processo.

Coadunando com o entendimento no que tange a complexidade da produção de provas no mundo digital moderno, Giova (2011, p. 1) explica que é essencial que as provas digitais só sejam aceitas como válidas em tribunal ou processo se a cadeia de custódia puder assegurar exatamente qual foi a prova, porquê ter sido coletada e analisada e como os dados probatórios foram recolhidos, analisados e comunicados. Ademais, Ćosić, Ćosić e Bača (2011, p. 3) afirmam que o peso probatório das provas digitais só pode ser salvaguardado se for possível provar a exatidão dos registros, para isso a cadeia de custódia das provas digitais deve ser mantida.

Antes de tudo, vale salientar que coleta de provas digitais é evidentemente diferente da coleta de provas tradicionais ou físicas. A distinção é tão significativa que as regras para as antigas investigações muitas vezes não fazem mais sentido para as novas (Kerr, 2005, p. 280). Não é coerente buscar recolher documentos físicos ou coletar depoimento de testemunhas oculares, por exemplo, já que frequentemente os crimes ocorrem dentro do contexto digital e as regras e normativas antigas já não se aplicam a esse contexto em diversos aspectos. Há necessidade de uma cadeia de custódia específica para obtenção da prova digital.

Cadeia de Custódia, segundo o *National Institute of Justice* (NIJ)[13], conforme disposto em seu glossário, nos Estados Unidos, é o registo das pessoas que tiveram a posse física das provas e o processo utilizado para manter e documentar o histórico cronológico das provas. O *National Institute of Standards and Technology* (NIST)[14] nos Estados Unidos diz que se trata de um processo e registo que mostra quem obteve as provas; onde e quando as provas foram obtidas; quem garantiu as provas; e quem tinha o controle ou a posse das provas. Define também que a "sequenciação" da cadeia de provas segue a seguinte ordem: (i) recolha e identificação; (ii) análise; (iii) armazenamento; (iv) preservação; (v) apresentação em tribunal; (vi) devolução ao proprietário. Há também que se mencionar o *Committee on National Security Systems*, que em seu glossário[15] (CNSSI 4009) também traz uma definição, que também é abordada pelo NIST (NIST SP 800-101 Rev.1), no qual explica exatamente que a Cadeia de Custódia é um processo que rastreia o movimento de provas através do seu ciclo de vida de recolha, salvaguarda e análise, documentando cada pessoa que manuseou as provas, a data/hora em que foram recolhidas ou transferidas, e o objetivo de quaisquer transferências.

Ćosić, Ćosić e Bača (2011, p. 3) também definem como o controle preciso do material de prova original pode ser potencialmente utilizado para fins legais. E Lima (2020, p. 251) diz que se trata de um mecanismo que visa garantir a autenticidade das provas auferidas, de forma a assegurar que dizem respeito especificamente ao que se investiga, não tendo sido adulteradas em nenhuma hipótese.

Frente aos conceitos listados, é possível perceber que Cadeia de Custódia se refere não apenas ao processo forense seguro de obtenção de uma prova que deve ser seguido para que ela esteja apta ao uso em juízo, mas também se refere à documentação completa de todas as fases que a evidência percorreu até que se transformasse em uma prova efetiva. Dessa forma, para que se obtenha efetiva fiabilidade de uma prova digital, é necessária uma cadeia de custódia bem definida, que cuide de todos os processos relativos à obtenção da prova, mantendo um histórico fidedigno e que permita a manutenção da integridade da evidência que se pretende utilizar. Vale esclarecer que, como esse trabalho se refere- às provas digitais de forma geral, o conceito de cadeia de custódia deve considerar todas as áreas jurídicas que requerem algum tipo

[13] Disponível em: https://nij.ojp.gov/nij-hosted-online-training-courses/crime-scene-and-dna-basics-forensic-analysts/glossary#:~:text=Chain%20of%20Custody,chronological%20history%20of%20the%20evidence. Acesso em: 04 dez 2023.
[14] Disponível em: https://csrc.nist.gov/glossary/term/chain_of_evidence. Acesso em: 09 dez 2023
[15] Disponível em: https://www.cnss.gov/CNSS/issuances/Instructions.cfm. Acesso em: 09 dez 2023

de prova digital (Criminal, Cível, Trabalhista, Tributária etc.), uma vez que não se trata de uma particularidade observada apenas no contexto criminal.

No que se refere aos direcionamentos relativos a uma efetiva Cadeia de Custódia de Prova Digitais, não há uma padronização nem das fases do processo forense e nem mesmo das informações que a documentação deve conter. Mas, há sentido em levar em consideração algumas diretrizes e regulamentações que tratam do assunto, para compreender pelo menos de forma geral o que se espera minimamente de uma Cadeia de Custódia.

O primeiro documento a ser citado foi produzido pela *Internet Engineering Task Force* (IETF), RFC 3227, de Título "*Guidelines for Evidence Collection and Archiving*[16]" (Brezinski, Killalea, 2002) no qual há o direcionamento principiológico de que o procedimento de coleta de provas digitais deve ser detalhado e os métodos utilizados os mais transparentes e de fácil reprodução possível, ou seja devem ser tão ágeis que qualquer pessoa que o reproduzir seja capaz de chegar ao mesmo resultado.

Diante das definições anteriormente expostas, em relação à Cadeia de Custódia, há quatro pontos informativos que a documentação do processo deve conter que são levantados, os quais são: (i) onde, quando e por quem a prova foi descoberta e coletada; (ii) onde quando e por quem a prova foi manipulada ou examinada; (iii) de quem era a custódia da prova e por quanto tempo. Como foi guardada; (iv) quando a prova mudou de custódia, quando e como a transferência ocorreu. Não há indicação específica de fases que devem ser seguidas.

O segundo documento que aqui se lista é a ISO 27037 - *Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence*[17], que está em vigor no Brasil desde 2014, sendo a ABNT ISO/IEC 27037:2013[18] a norma equivalente. Não diferente do documento anterior há antes de tudo a disposição de princípios no que se refere a coleta das provas para os fins de investigação, os quais são: (a) Pertinência, no qual deve estar demonstrada a relevância do material adquirido para a investigação; (b) Fiabilidade, em que os processos utilizados no tratamento de potenciais provas digitais devem ser auditáveis e

[16] BREZINSKI, D.; KILLALEA, T. Guidelines for Evidence Collection and Archiving. IETF. Online, 2002. Disponível em: https://www.ietf.org/rfc/rfc3227.txt Acesso em: 04 dez 2023.
[17] International Organization for Standardization (ISO), ISO/IEC 27037:2012 - Information Technology: Guidelines for Identification Collection Acquisition and Preservation of Digital Evidence. 2012.
[18] ISO/IEC 27037. Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 27037:2012 - Tecnologia da informação - Técnicas de segurança: Diretrizes para identificação, coleta, aquisição e preservação de evidência digital. 2013.

repetíveis; e (c) Suficiência, onde os responsáveis pelo manuseio das provas devem levar em consideração a coleta suficiente de materiais que permitam a realização da investigação (ABNT, 2013).

Diante do que foi exposto, no que se refere às informações que devem ser encontradas no documento referente a Cadeira de Custódia estão: (i) Identificador único de provas; (ii) Quem acendeu aos elementos de prova e a hora e local em que tal ocorreu; (iii) Quem registou a entrada e a saída das provas da instalação de conservação de provas e quando ocorreu; (iv) Por que razão as provas foram verificadas (qual o caso e o objetivo) e a autoridade competente, se aplicável; e (v) Quaisquer alterações inevitáveis as potenciais provas digitais, bem como o nome da pessoa responsável e a justificação para a introdução da alteração. Em relação as fases, destacam-se quatro: Identificação, Coleta, Aquisição e Preservação.

Na identificação há a procura, o reconhecimento e a documentação de potenciais provas. Aqui os suportes de armazenamento digital e dispositivos de processamento são identificados, e as potenciais provas digitais relevantes para a investigação são mapeadas. Há também o estabelecimento da ordem de prioridade de cada prova a ser coletada com base na volatilidade de cada uma, de forma a ter um processo de aquisição efetivo (ISO, 2012, 8).

Na coleta, os dispositivos que podem conter potenciais provas digitais são removidos do seu local original para um laboratório ou outro ambiente controlado para posterior aquisição e análise. Vale ressaltar que o documento prevê dois estados para os dispositivos que contêm potenciais provas digitais: quando o sistema está ligado ou quando o sistema está desligado. A depender do estado são aplicadas abordagens diferentes, entretanto de toda forma deve ocorrer documentação de toda a abordagem, bem como a embalagem destes dispositivos antes do transporte (ISO, 2012, 9).

Na aquisição, há produção de cópia das provas digitais, bem como a documentação dos métodos e das atividades realizadas para isso. O método de aquisição deve ser pormenorizado, uma vez que devem ser passíveis de reprodução posterior. Em caso excepcional de impossibilidade de repetibilidade do mesmo método depois, o perito deve justificar na documentação a razão da escolha do método (ISO, 2012, 9). Por fim, na preservação é o momento no qual se garante a utilidade de tudo que foi colhido para uma investigação. Esse processo envolve a proteção das potenciais provas, e dos dispositivos que as mantêm, devendo ser mantido em todas as fases de processamento das provas digitais (ISO, 2012, 10).

O terceiro documento que merece atenção é o "*Guide to Integrating Forensic Techniques into Incident Response - Recommendations of the National Institute of Standards and Technology*[19]" do NIST, no qual estão listadas quatro fases básicas: Coleta, Exame, Análise e Relatório. A coleta envolve a identificação, rotulagem, registo e aquisição de dados das possíveis fontes de dados de dados relevantes. O exame é o processamento forense dos dados recolhidos através de uma combinação de métodos automatizados e manuais, avaliando e extraindo dados de interesse particular. Na análise, há verificação dos resultados da fase anterior utilizando métodos e técnicas legais para obter informações úteis que respondam às questões que motivaram a coleta e o exame. Por fim, o relatório expõe os resultados da análise, que pode incluir a descrição das ações utilizadas, explicar como foram selecionados os instrumentos e procedimentos, determinar que outras ações devem ser aplicadas, e fornecer recomendações para melhorar as políticas, os procedimentos, as ferramentas e outros aspectos do processo forense.

Da análise dos três documentos é possível perceber que alguns pontos similares, primeiro referente a principiologia da cadeia de custódia, que sempre deve seguir o máximo de detalhamento possível, deve ser de fácil de fácil repetição posterior e as provas obtidas e os métodos utilizados devem ser evidentemente necessários ao processo de investigação. No que diz respeito as informações que a documentação que a cadeia de custódia deve ter, há que se identificar onde a prova foi obtida, quem teve acesso a ela, como foi coleta e o que foi extraído do processo.

Esses passos listados coadunam exatamente com a observação feita por Ćosić, Ćosić e Bača (2011, p. 3) ao explicar que para provar uma cadeia de custódia, deve-se saber cada detalhe de como a evidência foi processada em cada passo. Sendo a fórmula antiga utilizada por jornalistas, policiais e pesquisadores – "Os Cinco Ws" (Who, What, When, Where, Why, and How) – apropriada para aplicação na Cadeia de Custódia da Prova Digital.

Por fim, no que se referem as fases que devem compor o processo forense da Cadeia de Custódia há que se levar em consideração pelo menos a existência de três momentos específicos (i) identificação e coleta, onde os dados e evidências serão escolhidos e posteriormente recolhidos para compor a produção da prova; (ii) Aquisição e Exame, onde os

[19] KENT, Karen; CHEVALIER, Suzanne; GRANCE, Tim; DANG, Hung. Guide to Integrating Forensic Techniques into Incident Response - Recommendations of the National Institute of Standards and Technology. NIST. Online, 2006. Disponível em: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-86.pdf. Acesso em:09 dez 2023

dados obtidos serão processados mediante atualização de métodos diversos e as provas serão produzidas, e (iii) Análise e Preservação, onde os resultados obtidos serão avaliados e direcionados para a melhor forma de preservação.

No que se refere a direcionamentos referente a Cadeia de Custódia de Provas o Brasil tem a Lei n° 13.964/19 (“Pacote Anticrime) que evidencia dez etapas: (i) reconhecimento, (ii) isolamento, (iii) fixação, (iv) coleta, (v) acondicionamento, (vi) transporte, (vii) recebimento, (viii) processamento, (ix) armazenamento, (x) descarte[20]. Analisando cada fase é possível perceber que de certa forma estão contidas nas fases principais que listamos anteriormente.

Ocorre que a referida lei define Cadeia de Custódia como o conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte. Tendo o vestígio como o objeto dessa cadeia. O legislador brasileiro, entretanto, definiu vestígio da seguinte forma: “todo objeto ou material bruto, visível ou latente, constatado ou recolhido, que se relaciona à infração penal.”

Trazendo aqui as características da prova digital que foram anteriormente listadas, imaterialidade, a volatilidade ou fragilidade e alto potencial dispersão, não é tão fácil incluir as provas digitais como vestígios nos termos que a lei dispõe. Isso, porque conforme Dário José Kist (2019, p. 119) as características das provas digitais, especialmente a volatilidade, demandam uma abordagem e tratamento técnico qualificados para sua produção, devendo contar rigorosa metodologia em sua cadeia de custódia, sob pena de alteração ou perda. Há, portanto, necessidade de um regime jurídico específico que contemple as provas digitais considerando suas particularidades e as demandas que requer.

Essa necessidade é inclusive evidenciada na jurisprudência, uma vez que apesar das provas digitais já estarem sendo uma realidade em diversos casos e situações, há poucas discussões que mencionam a Cadeia de Custódia da Prova Digital. No âmbito do Supremo Tribunal Federal – STF há apenas a Decisão Monocrática no *Habeas Corpus* n° 17557/PR[21],

---

[20] Artigo 158-B da Lei n° 13.964/19 (Pacote Anticrime) Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689compilado.htm. Acesso em 03 dez 2023.

[21] BRASIL. Supremo Tribunal Federal (2. Turma). Agravo Regimental no Habeas Corpus 171.557 – PR. Agravo Regimental No Habeas Corpus. Processo Penal. ART. 22 da lei n. 7.492/1986. Alegação de quebra da cadeia de custódia das provas e ilicitude probatória. Impossibilidade de reexame do quadro fático-probatório na via eleita.

que tratou de denúncia realizada pelo Ministério Público contra operadores do mercado de câmbio negro que teriam utilizado contas mantidas no *First Curação International Bank* (FCIB), nas Antilhas Holandesas, para prática de operações dólar-cabo, ou seja, transferências internacionais informais. A denúncia, entretanto, esteve fundamentada em documentos e arquivos recebidos pelo Ministério Público em cooperação jurídica internacional. Em sede de defesa foi alegada justamente a suposta quebra de cadeia de custódia, conforme a seguir se expõe:

> Os arquivos digitais, como os que foram repassados pelas autoridades holandesas e que foram aportados nos feitos da Operação 'Curaçao'*, são especialmente suscetíveis a qualquer tipo de alteração, nas mais diversas fases, o que implica em uma demasiada fragilidade e grande facilidade de adulteração entre a fonte originária da prova e o material juntado aos autos. Daí que a preservação de uma cadeia de custódia adquire uma sensibilidade redobrada quando o caso envolver a coleta digital de provas***. Significa a necessidade de um standard de confiabilidade e originalidade da prova, que permitirá a verificação e refutação do fato histórico original e sua comprovação empírica, embargando qualquer filtro no material. Por conseguinte, cabe a esta Corte combater a presente ilegalidade no regime legal da prova, uma vez que não demonstrada, pela acusação, a preservação da cadeia de custódia no caso em questão, fato que deu origem à investigação preliminar que, por fim, resultou na condenação. (Brasil, 2023) (grifos do autor).

O Tribunal Regional Federal da Quarta Região - TRF4, entretanto, não considerou que houve indício de quebra de cadeia de custódia, baseando-se principalmente na "presunção de legitimidade" dos atos das autoridades envolvidas, o que fez com que os acusados impetrassem Habeas Corpus no STF que na ocasião foi negado pela Ministra Relatora Carmen Lúcia sob o argumento de que:

> Na espécie, para rever o entendimento firmado nas instâncias antecedentes, *seria necessário realizar novo cotejo da prova questionada* com o laudo pericial referido pelo agravante e afastar a autenticidade confirmada pelas autoridades que a avaliaram, o que *demandaria o reexame do contexto fático-probatório dos autos, inviável na via do habeas corpus* (Brasil, 2023) (grifos do autor).

Do exposto fica evidente a grande lacuna legislativa no que se refere a Cadeia de Custódia da Prova digital, uma vez que tendo um processo forense definido, os tribunais teriam tido condições de avaliar de forma mais adequada e coerente se a cadeia de custódia foi preservada, uma vez que a "presunção de legitimidade" das autoridades estatais por si só não afastam qualquer tipo de legalidade envolvendo o processo de manuseio de prova. Na verdade, a falta de uma normativa específica pode dar margem a arbitrariedades.

Precedentes. Agravo regimental ao qual se nega provimento. Agravante: Hussain Said Mourad. Agravado: Superior Tribunal de Justiça. Relator: Min. Cármen Lúcia, 18 de outubro de 2023. Diário de Justiça Eletrônico, 1 dez. 2023.Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=773144078. Acesso em 09 dez 2023.

No âmbito do Superior Tribunal de Justiça – STJ já há mais alguns casos como o *Habeas Corpus* n° 435.813/SP[22], no qual alegava o impetrante que o condenado, se encontrava cumprindo pena mediante sentença baseada em prova digital "que não se conhece a fonte, ou que mesmo conhecendo a fonte, esta não foi devidamente custodiada para preservar sua integridade", ademais ainda sustentou que:

> [A] prova digital é dotada de efemeridade, precariedade, não durabilidade, instabilidade, imaterialidade, complexidade, o que torna, pela extraordinária dificuldade intrínseca à espécie, inviável determinar, com rigor, que dados foram acrescentados, modificados ou suprimidos, não sendo possível portanto, demonstrar "prejuízo", confrontando eventual "prova íntegra" com "prova alterada" (pela perda da originalidade), sendo, assim, a falta de custódia adequada da prova a ser periciada e a quebra da cadeia de custódia da prova, a torna inadmissível no processo dentro do contexto das nulidades. (Brasil, 2018)

Em sua decisão Ministro Rogerio Schietti Cruz julgou "manifestamente improcedente", apenas ratificando os argumentos da sentença condenatória, no qual negava o abalo da prova e não reconhecia o "laudo" de mera opinião profissional como perícia. Outra ementa relevante a ser citada é a do Agravo Regimental no *Habeas Corpus* n° 803700/RS[23] do STJ que dispõe exatamente o que se segue:

> AGRAVO REGIMENTAL NO HABEAS CORPUS. ASSOCIAÇÃO PARA O TRÁFICO DE DROGAS. EXCESSO DE PRAZO. SUPRESSÃO DE INSTÂNCIA E PREJUDICIALIDADE. QUEBRA DA CADEIA DE CUSTÓDIA. NULIDADE NÃO CONSTATADA. PRISÃO PREVENTIVA. FUNDAMENTAÇÃO VÁLIDA. AUSÊNCIA DE ILEGALIDADE.
> [...]
> 2. "*Não há falar em nulidade decorrente da inobservância da cadeia de custódia pelas instâncias ordinárias, na medida em que a defesa não apontou nenhum elemento capaz de desacreditar a preservação das provas produzidas, conforme bem destacado no acórdão impugnado. Por certo, desconstituir tal entendimento demandaria o reexame de conjunto fático e probatório, inviável em sede de habeas corpus*." (AgRg no HC n. 810.514/SP, relator Ministro Ribeiro Dantas, Quinta Turma, julgado em 26/6/2023, DJe de 29/6/2023.)
> 3. Na espécie, *o Tribunal de origem asseverou a ausência de indicação concreta de prejuízo à defesa ou de adulteração com relação às provas digitais, colhidas pela autoridade policial, com o "cuidado de armazenar, categorizar e disponibilizar os*

[22] BRASIL. Superior Tribunal de Justiça. Habeas Corpus 435.813– SP. Impetrante: Luiz Antonio Zuliani. Impetrado: Tribunal Regional Federal da 3ª Região. Relator: Min. Rogerio Schietti Cruz, 07 de fevereiro de 2018. Diário de Justiça Eletrônico, 8 fev. 2018. Disponível em: https://processo.stj.jus.br/processo/monocraticas/decisoes/?num_registro=201800259473&dt_publicacao=09/02/2018. Acesso em 09 dez 2023.

[23] BRASIL. Superior Tribunal de Justiça (6. Turma). Agravo Regimental no Habeas Corpus 803.700– RS. Agravo regimental no habeas corpus. Associação para o tráfico de drogas. Excesso de prazo. Supressão de instância e prejudicialidade. Quebra da cadeia de custódia. Nulidade não constatada. Prisão preventiva. Fundamentação válida. Ausência de ilegalidade. Agravante: Gabriel Robeck. Agravado: Ministério Público Federal e Ministério Público do Estado do Rio Grande do Sul. Impetrado: Tribunal de Justiça do Estado do Rio Grande do Sul. Relator: Min. Jesuíno Rissato (Desembargador Convocado do TJDFT), 28 de agosto de 2023. Diário de Justiça Eletrônico, 30 ago. 2023. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202300513099&dt_publicacao=30/08/2023. Acesso em 09 dez 2023.

> *dados", após devida autorização judicial de quebra de sigilo telefônico*. [...] (Brasil, 2023) (Grifo nosso)

Nesse caso específico é possível perceber decisão muito próxima da que foi tomada no caso do STF anteriormente citado, novamente a impossibilidade de realizar reexame do conjunto fático em sede de *Habeas Corpus*. Entretanto, analisando todos os casos até agora expostos, há que se compreender que o judiciário não poderá justificar indefinidamente suas decisões relativas à cadeia de custódia da prova digital dessa maneira. Há necessidade de se definir um processo específico forma a atestar definitivamente a validade ou não da prova digital, compreendendo todo seu processo de obtenção e garantindo a segurança jurídica processual.

4 PROVA DIGITAL AUTOMATIZADA

Trazer à tona o grande desenvolvimento tecnológico e o aumento da dispersão e produção de dados, sem falar de suas consequências para o crescimento da Inteligência Artificial seria incoerente. Uma vez que exatamente em razão da existência de máquinas mais avançadas e melhor equipadas, além da grande quantidade de dados disponíveis é que a Inteligência Artificial tem alcançado grandes resultados e tem ganhado tanta notoriedade.

Ford (2021, p.6) compara esse desenvolvimento da Inteligência Artificial como a nova eletricidade, já que tem influência sobre diversos setores e a com propagação cada vez mais ampla. Uma vez que, não há mais nenhuma área que não esteja sendo minimamente influenciada ou submetida a atividades de inteligência artificial. Christian (2021, p. 11-12) nessa mesma toada, em seu famoso livro "*The Alignment Problem*", chega a dizer que há uma sensação crescente de que cada vez mais o mundo está entregue a Inteligência Artificial e eles estão progressivamente substituindo tanto as atividades mecânicas de softwares explicitamente programados quanto atividades humanas.

Então, não seria prudente pensar que a Inteligência Artificial não respingaria no contexto jurídico e especificamente na produção probatória. Conforme explica Fenoll (2018, p.14), apesar da pouca doutrina a respeito e boas bibliografias direcionadoras, seria como fechar os olhos para realidade pensar que Inteligência Artificial não pode ser aplicada em matéria judicial. Isso porque a IA vem não somente como uma ferramenta que pode dar celeridade aos processos investigativos, mas também como um instrumento que pode trazer evidências que eventualmente não seriam acessadas em uma simples investigação humana. Além de abarcar

de forma muito coesa a realidade de grande produção de dados, conseguindo analisar mais informações do que o próprio cérebro humano seria capaz.

Daqui em diante quer-se trazer a discussão não somente sobre a existência de provas digitais, advindas diretamente do influxo da tecnologia no cotidiano humano e do consequente desenvolvimento de uma sociedade digital, mas da realidade de automatizar a produção e a obtenção dessas provas.

É fundamental explicar que a automatização de processos administrativos e judiciais não é por si só uma ideia nova ou completamente infundada, segundo Langford (2020, p. 141) ela remonta pelo menos por volta da década de 1970, tendo como base a semelhança entre a lógica dedutiva do direito e a programação informática, em que os primeiros protótipos e aplicações começaram a ser desenvolvidos. Em 1972 na Noruega, por exemplo já se tinha notícias do uso de decisões automatizadas[24] para calcular as prestações ao abrigo da legislação sobre habitação (Langford, 2020, p. 141).

Atualmente, já é possível perceber que para além da digitalização se processos há também a automatização (Langford, 2020, p. 142), isso porque a tecnologia tem permitido uma diversidade de facilidades jurídicas, como a identificação de documentos e análise de textos, que não somente aceleram, como também e principalmente agregam novas possibilidades a prestação jurisdicional. O que não seria diferente em relação a produção de provas, uma vez que por si só as provas digitais têm suas limitações para uma efetiva obtenção e validade no uso processual e trazer um meio de automatização de sua coleta e produção poderia efetivamente auxiliar na construção de uma cadeia de custódia segura, bem como facilitar de forma significativa a obtenção de evidências em casos que de outra forma estariam sem suporte fático.

Nesse aspecto específico, Mitchell (2010, p. 35) explica que há pelo menos três desafios principais na obtenção de provas digitais, ou Perícia Digital ("*Digital Forensics*"), como a maioria dos autores se refere, que são: (a) o crescimento exponencial da capacidade de armazenamento, em unidades individuais unidades; (b) o crescimento dos sistemas distribuídos e as formas sofisticadas de ataque que podem atualmente ser lançadas, e (c) o grau de sofisticação técnica empregue pelos oponentes e a aparente incapacidade das ferramentas e

[24] "As decisões exclusivamente automatizadas correspondem à capacidade de tomar decisões através de meios tecnológicos e sem intervenção humana". WP29 – Grupo de Trabalho do Artigo 29 para a Proteção de Dados. Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679. Adotadas em 3 de outubro de 2017, com a última redação revista e adotada em 6 de fevereiro de 2018. Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection_pt. Acesso em: 30 set. 2023.

metodologias existentes e metodologias existentes para acompanhar o ritmo. Frente a eles, o autor explica que abordagens convencionais intensivas e manuais por si só não são capazes de de lidar com todos os problemas postos de forma célere e efetivamente suficiente. Sendo exatamente por isso que a Inteligência Artificial se mostra como uma saída viável e coerente nos processos de obtenção de prova.

4.1 Prova Digital Automatizada ou Perícia Forense Inteligente, Conceito e Ferramentas de Produção

Inicialmente, é crucial explicar que o termo "Prova Digital Automatizada" não é comum, nem mesmo há trabalhos com essa terminologia específica. Não há exatamente uma discussão definitiva no Brasil sobre esse assunto, mas é fundamental trazer a pauta às análises jurídicas o quanto antes, sendo exatamente a proposta principal dessa pesquisa.

Analisando as doutrinas internacionais é possível achar definições em trabalhos que falam sobre o processo forense de obtenção provas digitais ou perícia em relação as provas digitais ("*Digital Forensics*"), em que há a busca pela automação desse processo por meio da Inteligência Artificial. Nesses, é possível achar tímidas definições para o que seria uma prova digital automatizada, mas somente depois de analisar as discussões em torno da Perícia Forense Inteligente ("*Intelligent Forensics*") ou Perícia Automatizada ("*Digital Forensics Automation*"), uma vez que boa parte não se refere diretamente as provas, mas sim ao seu meio dwe obtenção.

Vale explicar brevemente que a Perícia ou Investigação Digital ("*Digital Forensics*") seria exatamente a ciência que permite encontrar determinados fragmentos de provas nos suportes digitais, mediante a preservação, coleta, análise e registro de um ambiente digital por razões legais (Dunsin *et al.*, 2022, p. 281). Irons e Lallie (2014, p. 590) também explicam que se trata de um conhecimento que tem valor para a aplicação da lei ou outras agências de investigação, tendo sido recolhido através da análise forense e do processamento de sistemas de armazenamento digital. É exatamente o processo de obtenção de provas digitais em que se leva em consideração uma cadeia de custódia bem definida, de forma a integrar posteriormente ao processo judicial.

A Perícia Digital Inteligente, então, seria aplicação dessa ciência por uma máquina, sem nenhuma interferência humana. Jarrett e Choo (2021, p.9) falam que a utilização da IA na investigação forense digital permite que os peritos forenses humanos encontrem respostas a questões de importância jurídica em menos tempo e com menos custos, além de trazer evidentes

possibilidades na limitação de riscos e desafios futuros, analisando minuciosamente evidências digitais atuais e antigas.

Irons e Lallie (2014, p. 590) explicam que a investigação forense inteligente se trata de uma abordagem interdisciplinar que utiliza os avanços tecnológicos e aplica os recursos de uma forma mais inteligente para resolver uma investigação. Sendo uma forma célere e autônoma para busca de evidências, mediante o uso direto de tecnologia, podendo ser utilizada de forma preventiva ou reativa.

Adam e Varol (2020, p. 1) também sustentam que a Investigação Digital Inteligente de Crimes se centra na exploração de conjuntos de dados históricos sobre crimes utilizando técnicas de extração de dados e técnicas de aprendizagem de máquina tanto para a investigação como para prevenção de crimes, o que envolve vários tratamentos diferentes dos dados.

Do exposto, então, é possível compreender que a prova, obtida de uma investigação conduzida por uma máquina, que analisou uma quantidade significativa de evidências, para solução de um caso específico, fazendo ligações e combinações, sem nenhuma interferência humana direta, seria o que aqui chamamos de prova digital automatizada. Podendo, então ser produzida tanto de forma preventiva, antes da ocorrência de qualquer infração específica, como de forma reativa, após a existência de um crime propriamente dito.

Jarrett e Choo (2021, p.9) mediante uma revisão literária, listaram as formas específicas em que a Inteligência Artificial poderia ser utilizada no contexto de produção de provas, que a seguir reproduzimos:

> Rastrear as provas de uma forma mais avançada e simplificada para conduzir uma investigação aprofundada. Identificar provas forenses críticas e torna-as passíveis de análise posterior objetiva e reproduzível. A avaliação da qualidade e da eficácia global dos métodos de investigação forense e a subsequente normalização desses métodos. Agilizar a pesquisa e a identificação de tendências importantes a partir de grandes volumes de dados, seguida da visualização dos visualização dos resultados. Auxiliar na interpretação desses resultados, revelando tendências e padrões que antes eram desconhecidos (Jarret; Cho, 2021, p. 9)[25].

[25] Tradução livre de: "*Tracing the evidence in a more enhanced and streamlined fashion to conduct an in-depth investigation (Franke & Srihari, 2008). It identifies critical forensic evidence and renders it to further analysis objectively and reproducible (Franke & Srihari, 2008). Assessing forensic investigation methods' overall quality and effectiveness and subsequently standardizing these methods (Franke & Srihari, 2008). Expediting the search and identification of important trends from large volumes of data followed by visualization of the results (Franke & Srihari, 2008). Assisting in the construal of these results reveals trends and patterns that were previously unknown (Franke & Srihari, 2008)*" (Jarret; Cho, 2021, p. 9).

A partir das poucas discussões voltadas para produção automatizada de provas digitais, há diversas ferramentas de Inteligência Artificial que são atualmente utilizadas para esse fim, com capacidades próprias e limitações, mas que tem como objetivo produzir prova a partir da análise de um ambiente ou contexto digital específico. A seguir listaremos algumas, que se enquadram nas formas listadas acima.

Os primeiros que listamos são os *Scrapers Softwares*, que são exatamente extratores de dados automatizados, normalmente muito utilizados no Facebook. Basicamente, há o rastreio da conta do Facebook de uma pessoa, há análise do conteúdo dos seus registros de atividade e esses dados são extraídos para um conjunto de dados estruturados (Bassil, 2019, p. 14). Para sua utilização deve estar vinculado a uma conta no Facebook, devendo o usuário indicar o conteúdo que deve ser coletado, depois das configurações realizadas a coleta é iniciada e o Scraper irá coletar as informações, salvando em um arquivo (Albino; De Lima, 2023, p.50). Ainda sobre esse tipo de ferramenta, Bassil (2019, p. 14), traz uma explicação técnica pertinente:

> O Facebook já lançou a Graph API para os programadores, a fim de facilitar a interação entre as aplicações de software e a plataforma do Facebook. Esta é uma REST API que pode ser utilizada para ajudar o extrator de dados. *Ela permitira recuperar interações e eventos sociais, entre uma variedade de outras tarefas que são valiosas para os investigadores forenses. Como resultado, a extração dos registos de atividade do Facebook pode ser feita de forma fiável* e sem problemas através da API Graph. (Bassil, 2019, p. 14) (Grifo Nosso)[26].

Trata-se, portanto, de uma ferramenta relevante para atividade forense e de produção de provas digitais, uma vez que é capaz de extrair dados diversos e cruzados, além de ser uma ferramenta segura.

A segunda é a *TweetBeaver* que, segundo Omezi e Jahankhani (2020, p. 261), se prova ser uma ferramenta muito útil em investigações forenses. Uma vez que oferece um conjunto completo de ferramentas analíticas, onde se pode procurar um utilizador, ver a quem está ligado, encontrar amigos comuns entre dois utilizadores etc. (Omezi, Jahankhani, 20200, p. 261). É utilizada para análise de conteúdo do *Twitter* (hoje conhecido como "X"), mediante a utilização de algoritmos de aprendizado de máquina para a análise de posts, comentários e curtidas, e

[26] Tradução livre de: "*Facebook has already released the Graph API for developers to ease the interaction between software applications and Facebook platform [17]. This REST-based API can be used to assist the data extractor. It would permit retrieving social interactions and events among a variety of other tasks that are valuable to forensics investigators. As a result, extracting Facebook Activity Logs can be done reliably and seamlessly via the Graph API*." (Bassil, 2019, p. 14).

assim rastrear as relações dos usuários, identificar o tipo de conteúdo vinculado, atividades suspeitas etc. (Albino; De Lima, 2023, p.50).

A terceira ferramenta a ser mencionada é o *MentionMap*, que não apenas permite ter acesso as pessoas com que um usuário mais tem conversas, mas também a forma como os usuários do *Twitter* se relacionam. Para obtenção dos resultados, deve ser introduzido o nome do usuário do Twitter e há a produção de um papa interativo de ligações[27]. Frente a essas possibilidades, pode ser uma ferramenta muito relevante para "investigações criminais, monitoramento de atividades maliciosas, análise de risco e outras finalidades" (Albino; De Lima, 2023, p.50).

As ferramentas citadas até aqui possuem uma particularidade interessante no que diz respeito especificamente a juntada de informações sobre um determinando indivíduo ou objeto e produzir prova com a junção das evidências coletadas. Entretanto, vale ressaltar que também existem ferramentas de Inteligência Artificial que são úteis na reconstrução de fatos com base em vestígios já existentes, sendo efetivamente relevantes em investigações (Fenoll, 2018, p. 26).

Uma delas é a *STEVIE*, que é uma ferramenta baseada na argumentação, destinada a apoiar a investigação criminal, de forma que os analistas de um caso possam visualizar provas e inferências sobre a situação investigada. (Nissan, 2017, p. 449). Trata-se então de um programa que a partir dos dados existentes relativos a um caso, constrói histórias coerentes do que pode ter ocorrido (Fenoll, 2018, p. 26). Muito útil em casos em que o entendimento sobre o ocorrido é muito obscuro, a produção de "histórias possíveis" pela IA, pode auxiliar não somente a chegada de uma conclusão sobre o caso, mas também no direcionamento das investigações e na busca por evidências específicas, justificando-as.

Há ainda três outros programas interessantes que dizem respeito a "modelação do raciocínio sobre provas jurídicas", que segundo Nissan (2017, p. 451), apenas recentemente surgiu como uma área significativa dentro do campo da Inteligência Artificial e Direito, quando antes existiam apenas modelos estatísticos de provas criminais. Dois deles são *ECHO* e *PEIRCE-IGTT*, que são capazes de elaborar hipóteses e estratégias de acusação e defesa de um

[27] Disponível em: https://thenextweb.com/news/mentionmap-is-a-cool-interactive-map-of-twitter-connections. Acesso em: 07 Jan 2024.
Disponível em: https://www.montsepenarroya.com/en/mentionmap-herramienta-visual-para-conocer-las-menciones-en-twitter/. Acesso em: 07 Jan 2024.

réu (Fenoll, 2018, p. 26). O *ECHO* é uma ferramenta baseada em redes neurais artificiais (Nissan, 2017, p. 451), e o *PEIRCE-IGTT* é um software de inferência abdutiva a partir da Inteligência Artificial (Nissan, 2017, p. 451). A outra ferramenta é a *ALIBI*, que segundo Nissan (2009, p. 13) trata-se de um *AI Planner* (planeador de IA) que se faz passar por uma pessoa que é acusada de algum delito, negando a acusação principal procurando a exoneração desta ou uma alternativa de responsabilidade menor (Nissan, 2017, p. 451).

Do exposto, se pode perceber que a Inteligência Artificial está mais próxima da produção probatória há mais tempo do que se poderia supor, abarcando não somente a coleta de evidências e realização de cruzamentos e inferências para produção da prova em si, como também o direcionamento da produção da prova no auxílio as demandas do réu e para um melhor convencimento do juiz, abarcando ambas as partes do processo judicial.

4.2 Casos Práticos de Obtenção das Provas Digitais Automatizadas

No que se refere a obtenção das provas as Inteligências Artificiais podem ser programadas e direcionadas de diversas formas. Carrier e Spafford (2005, p. 1) citam pelo menos duas delas, sendo a primeira a busca baseada em algum tipo de evidência preliminar, e a segunda a busca de termos, documentos e evidências específicas em um determinado campo investigativo. Então a máquina poderia ser levada a buscar evidências próximas ao modelo que já se tem, de forma a coletar tudo que remeter ao parâmetro indicado, ou a busca específica de termos, fotos, documentos, dados etc.

Como exemplos, podemos mencionar as IAs utilizadas nos Centros de Operações vinculados à Justiça Eleitoral, com sede na cidade de Menlo Park, na Califórnia, Estados Unidos, responsável por eliminar informações falsas sobre o processo eleitoral brasileiro. Rosina (2019)[28], no Seminário Internacional sobre "*Fake News* e Eleições", chegou a informar que no ano de 2019 já era possível "a partir da inteligência artificial, remover 99,6% das contas falsas, antes mesmo de elas serem denunciadas". Nesse caso, há busca de um conteúdo específico (*Fake News*) em um campo específico.

[28] ROSINA, Mônica. Seminário Internacional Fake News e Eleições [recurso eletrônico]: anais. Brasília: Tribunal Superior Eleitoral, 2019. p.177. Disponível em: https://www.tse.jus.br/hotsites/catalogo-publicacoes/pdf/livro-digital-fake-news.pdf. Acesso em: 07 Jan 2024.

Ademais, em 2022, a Faculdade de Direito de Vitória em seu relatório[29] da Missão de Observação Eleitoral (MOEs), apontou que o Tribunal Superior Eleitoral, em prática de parcerias com especialista nas áreas de Ciência da Computação e Tecnologia da Informação, "[...] está-se estruturando instrumentos de IA que poderão contribuir no avanço da gestão destas práticas, uma vez serem instrumentos que não serão excluídos dos processos eleitorais e outras práticas democráticas, mas, em perspectiva, deverão ser incrementadas" (Morais, 2023, p. 8). No mesmo relatório, houve inclusive menção a proposição de uma ferramenta de Inteligência Artificial cujo objetivo era exatamente identificar *Fake News* precocemente em mídias sociais:

> [...] por meio de uma classificação binária (notícia falsa/verdadeira) em uma perspectiva tríplice e simultânea *das relações entre o editor da notícia (fonte), a notícia em si e o usuário, explorando informações auxiliares de contexto que o próprio ecossistema das mídias sociais fornece*. Espera-se, assim, obter em tempo real a análise sobre a falsidade da notícia apontando a origem da fonte (usuário e URL), explicação do motivo da notícia ter sido rotulada como falsa, verificação do "sentimento" envolvido na postagem (neutro, positivo ou negativo), bem como outros dados relativos à postagem *para direcionar tais informações à Justiça Eleitoral auxiliando-a e munindo-a eficazmente no combate à disseminação de notícias falsas e punição dos responsáveis*. Assim, há um lado objetivo da ferramenta em que se observa a estrutura da linguagem e um outro lado em que se analisa elementos subjetivos, como sentimentos, para oferecer constatações mais assertivas acerca das classificações geradas em relação às semânticas dos textos analisados. Atualmente, já foi implementada na ferramenta a parte de análise de sentimento e estamos iniciando o desenvolvimento do módulo de detecção de Fake News em si, a parte mais objetiva do projeto (Morais, 2023, p. 9) (grifos do autor).

Do exposto, é possível perceber a presença real da Inteligência Artificial na produção de provas nos processos eleitorais brasileiros, gerando inclusive já consequências jurídicas aos indivíduos envolvidos em questões relativas às informações falsas. A razão legítima assenta-se na possibilidade de se dar uma rápida resposta a questões que podem impactar severamente na continuidade do processo eleitoral. A partir desse processo, mediante a juntada de evidências que comprovam os ilícitos, conteúdos foram retirados da circulação e a contas de usuários foram derrubadas, fatos que geram consequências jurídicas diretas.

Um outro caso interessante, que traz luz referente a análise comparativas realizadas por Inteligência Artificial, ocorreu no Reino Unido em 2016. Nessa situação, 36.000 estudantes internacionais tiveram seus vistos revogados com base no reconhecimento de voz humana realizado pela IA de uma empresa de serviços linguísticos contratada, que indicava que os

---

[29] MORAIS, Jose Luis Bolzan de. Missão de observação eleitoral: o controle, pela justiça eleitoral, do uso e impacto das redes sociais no processo eleitoral: relatório final. 2023. Disponível em: https://www.tse.jus.br/++theme++justica_eleitoral/pdfjs/web/viewer.html?file=https://www.tse.jus.br/eleicoes/eleicoes-2022/arquivos/missoes-de-observacao-eleitoral-nacionais/faculdade-de-direito-de-vitoria-ppgd-fdv/@@download/file/TSE-faculdade-de-direito-de-vitoria-ppgd-fdv.pdf. Acesso em: 07 Jan 2024.

estudantes tinham utilizado proxies nos testes de inglês necessários para obter os vistos (Mcauliffe, 2021, p. 6).

A situação começou em razão de uma investigação realizada pelo programa Panorama da BBC em 2014, que tornou os estudantes alvos do Ministério do Interior (o principal departamento governamental para a imigração e passaportes, política de drogas, crime, incêndios, contra-terrorismo e polícia no Reino Unido). Foi então descoberto uma fraude sistemática no *Test of English for International Communication* (TOEIC), que era utilizado para provar a proficiência na língua inglesa, um requisito para a obtenção de vistos. Foi pedido ao ETS (*English Testing Services*) que analisasse os ficheiros de som e investigasse se a acusação era verdadeira. Utilizando uma análise de voz automatizada, o ETS identificou 33.725 testes como "inválidos" e 22.694 como "questionáveis". Os testes inválidos resultaram na revogação dos vistos dos estudantes, que foram enviados de volta para casa. Os estudantes com testes questionáveis foram convidados para uma entrevista antes de serem tomadas quaisquer medidas. Com este processo, no final de 2016, então, os estudantes foram enviados para casa devido à revogação dos seus vistos.

Existem também formas um pouco mais intrusivas que envolvem análise de padrões e comportamentos, bem como a perfilização de indivíduos, tendo como resultado entrega de previsões e resultados nesse sentido. Conforme aponta Irons e Lallie (2014, p. 593), há uma diversidade de técnicas que podem ser aplicadas e conjuntamente relevantes nesse sentido, como por exemplo as redes neurais (“Neural Networks”) que podem ser treinadas para categorizar comportamentos apropriados (ou não), sendo capazes de modelar o comportamento de diferentes utilizadores de um mesmo domínio ou site, de modo a indicar padrões de utilização incomuns para o utilizador que está com sessão iniciada. A extração de dados (*Data Mining*) e outras técnicas de máquina podem ser utilizadas para descobrir padrões de comportamento e direcionar exceções.

Nesse contexto específico, vale trazer o exemplo do COMPAS, que é unanimemente citado em diversos trabalhos relativos ao uso de inteligência artificial, modelos preditivos, decisões automatizadas etc. Esse software foi largamente utilizado no sistema de justiça criminal nos Estados Unidos (Dorleon, 2023, p. 27) para definir penas e possíveis reincidência dos presos. Conforme informações[30], o programa trabalhava com um sistema de pontos em que

[30] Disponível em: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

são feitas várias perguntas e a partir delas atribuída uma nota ao preso. Então, mediante essa avaliação (nota) o juízo definia se haveria soltura, pagamento de fiança, prisão definitiva, ou outro tipo de sentença. A intenção norte-americana era exatamente dar maior objetividade às decisões judiciais. É possível perceber que os relatórios analíticos produzidos, tidos como provas, eram suficientes para ajudar no convencimento do juiz em relação aos casos e influenciar nas decisões.

Outro exemplo relevante, ocorreu na Nova Zelandia. Algumas notícias em 2018 trouxeram à tona o fato de que o órgão responsável pela imigração no país estaria utilizando dados como idade, sexo, etnia etc., dos imigrantes, para mapear grupos que geravam altos custos hospitalares ou que eram mais propensos a cometer crimes[31]. O órgão estava usando essas informações para decidir previamente qual indivíduo seria deportado, não lhes dando a chance de serem processados ou permitindo que voltassem a solicitar vistos. Ademais, em outra ocasião, mais análises foram feitas mapeando grupos demográficos que fizeram mais alegações fraudulentas no processo legal de imigração, de forma a dificultar a entrada desses grupos.

Para além das questões éticas que permeiam todos os exemplos mencionados, as quais serão abordadas mais adiante, tem-se que efetivamente a produção automatizada de provas existe e têm gerado consequências diretas aos indivíduos envolvidos, tendo sido efetivamente incorporadas não somente em questões processuais de diversas áreas legais, como a base de decisões relevantes, capazes de alterar significativamente as realidades que envolvem. Em relação aos processos eleitorais, contas derrubadas, advindas da seleção feita pela IA, podem afetar significativamente o trabalho de pessoas que trabalham na internet. Já em relação aos processos administrativos migratórios, a prova de fraude, baseada na análise da IA, gerou o fim da possibilidade de morar no Reino Unido para diversos estudantes. Na nova Zelandia, a perfilização tirou antes de tudo a possibilidade de se adquirir o visto. E no caso do Compass, no Estado Unidos, a condenação ou não de uma pessoa estava diretamente vinculada a prova produzida. Há, portanto, aplicação prática, e há consequências.

A análise desses grandes volumes de dados e as plataformas de computação de alto desempenho, podem levar ao desenvolvimento de sistemas que aprendem e melhoram

---

Acesso em: 07 Jan 2024.
Disponível em: https://www.bbc.com/portuguese/brasil-37677421. Acesso em: 07 Jan 2024.

[31] Disponível em: https://medium.com/o-centro-de-ensino-e-pesquisa-em-inova%C3%A7%C3%A3o-est%C3%A1/intelig%C3%AAncia-artificial-e-controle-migrat%C3%B3rio-algoritmos-podem-discriminar-migrantes-85d04d152440#_ftnref17. Acesso: 16 Abril 2023.

continuamente o desempenho das máquinas, de forma a acompanhar tendências em evolução no domínio da informática forense (Irons; Lallie 2014, p. 593). Assim, o processo de obtenção de provas automatizadas vai se tornando cada vez mais desenvolvido e aprimorado, bem como cada vez mais intrínseco na realidade judicial.

4.3 Questões Éticas e Normativas Advindas da Produção Automatizada da Prova

Conforme citamos anteriormente, a utilização da Inteligência Artificial na investigação forense digital permite maior celeridade na obtenção de resposta, menos custos, além da possibilidade de limitação de riscos futuros e problemas, mediante a análise prévia das provas digitais (Jarrett; Choo, 2021, p.9). Coadunando, inclusive, com o que diz Irons e Lallie (2014, p. 59), quando explicam que o que se espera da aplicação da Inteligência Artificial às investigações forenses digitais é o fornecimento de um conjunto útil de ferramentas para que o investigador resolva questões complexas, abarcando o grande volume de dados posto e dentro de um prazo razoável e direcionando o que for relevante.

Albino e Lima (2023, p.50) destacam 6 vantagens dessa aplicação inteligente na coleta de dados digitais das quais destacamos: (a) Eficiência, com o rápido processamento de grande volume de dados de forma célere; (b) Precisão, mediante a possibilidade do direcionamento específico na busca de padrões e tendências nos dados, que humanamente não seriam tão facilmente detectados; (c) Identificação de Informações Relevantes, em meio aos grandes conjuntos de dados; (d) Automação de Tarefas Repetitivas; (e) Armazenamento Seguro, garantindo a integridade da prova, sem alterações externas; e (f) Fundamentação para Tomada de Decisões, podendo auxiliar os juízes a direcionar suas decisões com base nas provas obtidas.

Do exposto, então é inegável que a Inteligência Artificial vem a agregar de sobremaneira na produção da prova digital, facilitando processos, encontrando provas de difícil acesso, dando predições preventivas e até mesmo diminuindo custos de investigações forenses com menos gasto de tempo. Ocorre que, não é possível ignorar o lado oposto de toda essa realidade, já que a Inteligência Artificial por si só não é uma matéria que atingiu a plena maturidade, além de ser extremamente mutante. Tal realidade, dá margem a consequências incertas e riscos não previstos que podem atingir diretamente garantias e direitos fundamentais. Além de estar sendo utilizada por quase todas as esferas sociais para os mais diversos fins.

Prado (2021, p. 173) diz que é inquestionável que a Inteligência Artificial suscita questões interessantes quando observadas pela ótica do devido processo legal. Acrescenta então

que:

> A «economia dos algoritmos» rege a vida moderna. E *incrementa riscos de toda ordem, não apenas à consecução do objetivo de produção de informações fiáveis e auditáveis que possam servir de base a decisões jurídico-penais de qualidade*, mas a «economia dos algoritmos» também preocupa pelo que significa em termos de uma *sociedade cada vez mais hipervigiada*. (Prado, 2021, p. 173) (grifos do autor).

Dessa forma, do mesmo modo que se deve considerar o valor da presença da Inteligência Artificial no contexto da produção probatória, com as diversas possibilidades aprazíveis, não se podem ser esquecidas as consequências negativas e os desdobramentos jurídicos que podem afetar a efetiva entrega do devido processo legal. Da análise breve de todos os casos anteriormente postos é possível identificar alguns questionamentos que direcionam para algum tipo de problemática relevante e que pode afetar a lisura da condução processual como também e principalmente a proteção de direitos fundamentais.

No caso relativo a Justiça Eleitoral Brasileira, com a retirada de conteúdos de "Fake News" da Internet, pode-se questionar qual seria o parâmetro usado para classificar uma informação como falsa? Está a Inteligência Artificial submetida a algum tipo de viés político? Qual a legitimidade das provas produzidas e qual o peso que impõem na responsabilização de um indivíduo? Análise de dados de pessoas que não são diretamente ligadas ao caso, sem seus consentimentos específicos, geraria alguma falha de privacidade?

Já na situação referente a migração no Reino Unido, inevitavelmente questiona-se: "quais os preconceitos intrínsecos a Inteligência Artificial de análise de voz?"; "onde estão as possibilidades de revisão daquela prova produzida pela máquina?"; "haveria possibilidade de responsabilização do Estado ou do desenvolvedor da Inteligência Artificial caso fosse posteriormente comprovado algum tipo de equívoco?"[32]; "qual o percentual de fiabilidade e confiabilidade dos resultados obtidos?".

Por fim, nos casos relativo à perfilização de pessoas (*Compass* e da nova Zelandia), há novamente questionamentos sobre quais seriam os parâmetros adotados aos softwares e sobre: "quais os viés adquiridos pela máquina?"; "de que forma a Inteligência Artificial chegou aos resultados obtidos?"; "qual o valor das predições como provas judiciais? Seriam legalmente legítimas e juridicamente apropriadas?"; "haveria possibilidade de uma revisão dos resultados obtidos?"; "os resultados desastrosos e controversos seriam passíveis de ações de

[32] Nesse caso do Reino Unido posteriormente foi efetivamente evidenciado que boa parte dos resultados obtidos por meio da Inteligência Artificial estavam errados e uma gama significativa de pessoas foi deportada injustamente.

responsabilização?”.

Dos questionamentos levantados fica evidente a quantidade de tópicos que precisam ser abarcados pelo direito relativos ao uso de Inteligência Artificial para produção das provas digitais de forma que estas possam ser efetivamente utilizadas de forma legítima e segura. Há que se passar a prova digital automatizada por dois tipos de admissibilidade, a normativa e a ética, para que então possa ser efetivamente entranhada ao processo contribuindo efetivamente com o devido processo legal, o que será efetivamente abordado no capítulo subsequente.

5 CONFORMIDADE ÉTICO-NORMATIVA NA PRODUÇÃO DA PROVA DIGITAL AUTOMÁTICA

Os avanços percebidos pela presença da tecnologia e inteligência artificial realmente não podem ser ignorados, nem muito menos barrados, uma vez que seria completamente contraproducente se negar ao uso de ferramentas que tanto têm a acrescentar e a facilitar o convívio social e a condução das atividades rotineiras. Por outro lado, não é coerente que sejam adicionadas de qualquer forma ao meio social e jurídico sem nenhum tipo de direcionamento normativo ou sem que se busque compreender efetivamente as consequências negativas e como fazer para minimizá-las.

Especificamente no que se refere a inserção Inteligência Artificial, Fenoll (2018, p. 14) explica que apesar da pouca doutrina e literatura sobre esse assunto, seria fechar os olhos para realidade acreditar que essa tecnologia não poderia ser aplicada em matéria judicial de forma ainda mais ampla do que já está implementada e do que se sabe. Ignorar todo esse panorama é prejudicial, uma vez que juntamente com tantas possibilidades, tantos outros riscos surgem (Prado, 2021, p. 186) e se apresentam como desafios diretos não somente à entrega efetiva dos direitos fundamentais, como também do acesso à justiça, a um devido processo legal e ao convívio social pacífico. Ainda sobre essa realidade tem-se que:

> As vantagens promovidas pelo uso dessas novas tecnologias são acompanhadas de novos problemas e riscos. Alguns desses riscos são epistêmicos e decorrem do próprio funcionamento dessas novas tecnologias, sobre o qual o operador jurídico normalmente pouco ou nada sabe. (Massena, 2019, p. 30)

No quesito ético e moral, é importante destacar que em grande parte os riscos (e problemas éticos) advindos de atividades com o uso de Inteligência Artificial não são consequência de um mau comportamento, como nos humanos, mas o resultado da falta de análise das consequências, da falta de monitoramento da IA “em estado selvagem” e da falta de conhecimento sobre ao que se ater ao desenvolver, adquirir e usar uma IA (Blackman, 2022, p.

7). A máquina recebe comandos, sendo direcionada a chegar a determinados resultados, sem, entretanto, analisar nada além e nada aquém do que lhe foi proposto, ela apenas tem como ponto focal realizar exatamente o que seu desenvolvedor a direcionou, não necessariamente da forma que se espera.

Um exemplo direto disso, foi dado por Christian (2021, p. 9-10) quando conta que Dario Amodei, pesquisador de um projeto chamado Universe, onde fazia parte de uma equipe que trabalha para desenvolver uma IA única e de uso geral que possa jogar centenas de jogos de computador diferentes com habilidade igual a humana. No caso, específico ele estava responsável por treinar a máquina em um certo jogo de regata de barcos, e na ocasião, de forma a sintetizar todos os comandos relativos a posição da pista, voltas, posicionamento frente a outros barcos, etc, ele apenas direcionou a máquina dizendo que havia um sistema de pontos. Pois bem, ao analisar a IA jogando percebeu que ela fez apenas o barco girar em círculos por horas apenas coletando "pontos". Aparentemente uma estratégia perfeita para executar o que tinha sido direcionada a fazer, mas não era esta especificamente a intenção de seu desenvolvedor. Claramente ele queria que a máquina fosse capaz de entender que deveria seguir na pista, ultrapassar outros barcos, coletar os pontos e então chegar em primeiro lugar.

Nesse exemplo anterior, a máquina não gerou especificamente nenhum dano, mas é possível observar que utilizou os "meios que entendeu" suficientes para realizar a tarefa e entregar exatamente o que foi comandada a fazer. O mesmo pode ocorrer em qualquer outra situação de aplicação prática da IA. E como visto, nem sempre os meios são adequados, ou muito menos previstos por quem a desenvolve.

Uma vez então que se está diante de uma realidade de impactos e resultados imprevisíveis, que muitas vezes podem trazer consequências irreversíveis ou de difícil retorno ao estado inicial, é preciso uma movimentação jurídica intencional para o efetivo direcionamento do uso, bem como para a manutenção das garantias constitucionais de cada indivíduo. Ressalta-se que, embora os riscos éticos não sejam novos - discriminação, invasão de privacidade, homicídio involuntário etc. – existindo há mais tempo do que se pode recordar, a Inteligência Artificial consegue criar formas novas de concretizar esses riscos (Blackman, 2021, p.7). O que significa que novas técnicas e mecanismos precisam ser implementados, de forma a impedir a concretização desses ilícitos.

Aqui há uma interseção entre a ética e o direito. Apesar do pensamento frequente de que a ética e o direito são distintos, há muita relação entre os deveres éticos e jurídicos. Isso, porque as normas jurídicas têm muitas vezes também uma vertente ética, além do que a ética pode (e tem), em certa medida, tornar-se uma espécie de *soft law* (Bartneck, 2021, p. 22). Então, antes que uma prova automatizada seja entranhada ao processo judicial é necessário não apenas que seja normativamente prevista, mas que também esteja adequada a um padrão ético mínimo para manutenção dos direitos fundamentais de cada indivíduo.

5.1 Admissibilidade ética

Mediante a análise dos casos mencionados no capítulo anterior (Ponto 4.2) é possível concordar que há pontos controversos que chamam a reflexão sobre diversos aspectos éticos. Dar atenção a esses aspectos por si só não irá resolver completamente todos os problemas advindos da inserção da Inteligência Artificial na produção probatória de provas, mas ajudará certamente a preservar direitos fundamentais e prevenir erros graves.

Especificamente quando se fala sobre princípios éticos para Inteligência Artificial, não há um consenso definitivo sobre quais são eles. Nas palavras Kieslich, Keller e Starke (2022, p.3): "Existe um consenso generalizado sobre a necessidade de uma IA ética, mas não sobre o seu aspeto concreto"[33].

Nessa perspectiva, trazendo o exemplo do documento produzido pelo Grupo Independente de peritos de alto nível sobre a inteligência artificial (*High-Level Expert Group on AI* - AI HLEG) criado pela Comissão Europeia em Junho de 2018, chamado de Orientações Éticas para uma IA de Confiança (*Ethics Guidelines for Trustworthy Artificial Intelligence*), onde trazem sete requisitos que os sistema de IA devem ter (ou cumprir) para serem considerados como fiáveis, são eles: (i) supervisão humana; (ii) robustez técnica e segurança; (iii) privacidade e governança de dados; (iv) transparência; (v) diversidade, não discriminação e justiça; (vi) bem-estar social e ambiental; (vii) responsabilidade (HLEG, 2019, p. 2).

Outro documento importante a ser citado é a Recomendação do Conselho em

[33] "There is a widespread agreement on the need for ethical AI, but not on what it should look like in concrete terms."

Inteligência Artificial (*Recommendation of the Council on Artificial Intelligence*[34]) da Organização para a Cooperação e Desenvolvimento Econômico (*Organisation for Economic Co-operation and Development* - OECD), que traz cinco princípios que os membros e não membros que aderirem a recomendação devem implementar a fim de promoverem a gestão responsável de uma IA fiável (OECD, 2021). São estes: (i) crescimento inclusivo, desenvolvimento sustentável e bem-estar; ii) valores centrados no ser humano e justiça; (iii) Transparência e explicabilidade; (iv) robustez, segurança e proteção; (v) responsabilidade (OECD, 2021).

No trabalho acadêmico de Jobin, Ienca, Vayena (2019) initulado "*Artificial Intelligence: the global landscape of ethics guidelines*" eles identificaram 84 documentos que contêm princípios éticos e diretrizes para Inteligência Artificial e da análise definiram onze princípios éticos gerais, comuns a quase todos os documentos: (i) transparência, (ii) justiça e equidade, (iii) não maleficência, (iv) responsabilidade, (v) privacidade, (vi) beneficência, (vii) liberdade e autonomia, (viii) confiança, (ix) dignidade, (x) sustentabilidade, (xi) solidariedade.

Em um outro trabalho parecido, Floridi et al (2021), da análise de seis documentos[35], buscaram oferecer uma síntese dos conjuntos de princípios existentes produzidos por várias organizações e iniciativas respeitáveis e com diversas partes interessadas. Nessa ocasião chegaram a um número de 47 princípios, que sintetizaram em cinco: (i) beneficência, relacionado ao bem-estar e a preservação da dignidade; (ii) não maleficência, relacionada a

---

[34] OECD (2021) Recommendation of the Council on Artificial Intelligence. Disponível em: https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449. Acesso em: 18 jan 2024.

[35] São estes os documentos analisados nesse trabalho:

1. The Asilomar AI Principles, developed under the auspices of the Future of Life Institute, in collaboration with attendees of the high-level Asilomar conference of January 2017 (hereafter "Asilomar"; Asilomar AI Principles 2017);
2. The Montreal Declaration for Responsible AI, developed under the auspices of the University of Montreal, following the Forum on the Socially Responsible Development of AI of November 2017 (hereafter Montreal; Montreal Declaration 2017);
3. The General Principles offered in the second version of Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems. This crowd-sourced global treatise received contributions from 250 global thought leaders to develop principles and recommendations for the ethical development and design of autonomous and intelligent systems, and was published in December 2017 (hereafter "IEEE; IEEE 2017);
4. The Ethical Principles offered in the Statement on Artificial Intelligence, Robotics and Autonomous Systems, published by the European Commission's European Group on Ethics in Science and New Technologies, in March 2018 (hereafter "EGE"; EGE 2018);
5. The "five overarching principles for an AI code" offered in paragraph 417 of the UK House of Lords Artificial Intelligence Committee's report, AI in the UK: ready, willing and able?, published in April 2018 (hereafter "AIUK"; House of Lords 2018); e
6. The Tenets of the Partnership on AI, a multistakeholder organisation consisting of academics, researchers, civil society organisations, companies building and utilising AI technology, and other groups (hereafter "the Partnership"; Partnership on AI 2018).

privacidade e a segurança; (iii) autonomia, relacionada ao poder de decidir; (iv) justiça e (v) explicabilidade.

Vale mencionar também Kieslich, Keller e Starke (2022) que apontam a transparência (ou explicabilidade), a equidade, a responsabilidade (prestação de contas), a privacidade, a não maleficência, a liberdade e a autonomia e a beneficência, como os sete princípios proeminentes quando se fala de inteligência artificial. Montoya e Rummery (2020, p. 6) apontam também que identificaram quatro desafios principais no que se refere a aplicação de IA, que são a equidade, a transparência, a explicabilidade e a responsabilização. Por fim, Blackman (2021) em seu livro ainda aponta que a ética em IA passa principalmente pela proteção da privacidade, a diminuição de vieses e a possibilidade da máquina exercer a explicabilidade de suas funções.

Do exposto, é possível observar alguns princípios comuns. Efetivamente todos os que foram citados são inequivocamente importantes para construção de uma IA fiável e responsável. Ademais, embora os autores tenham indicado esses princípios éticos para aplicação de IA de uma forma geral, é coerente nesse trabalho compreender que eles também são efetivos no que se refere a produção probatória automatizada, uma vez que os desafios que dão margem aos problemas éticos abarcados pelos princípios citados podem ser identificados nos casos apontados no capítulo anterior (Item 4.2). O presente trabalho então irá concentrar-se brevemente então em quatro princípios que entendemos fundamentais para entender a admissibilidade ética da prova digital automatizada, são eles: (a) Justiça; (b) Transparência; (c) Explicabilidade; e (d) Responsabilidade.

5.1.1 Justiça (Fairness)

O primeiro princípio que deve ser levado em consideração é o da justiça, normalmente citado nos trabalhos e pesquisa como *Fairness*. Está especificamente relacionado com a equidade que deve estar inserida no uso de Inteligência Artificial, em razão do frequente pensamento, equivocado, de que a máquina teria um trabalho mais objetivo. Na prática, entretanto, a "equidade" da máquina vai ser construída a partir dos dados fornecidos como input para seu aprendizado, e estes podem vir com diversos vieses (Choraś, 2020, p. 620). Conforme Simons (2023. p. 18) diz em sua pesquisa "uma máquina é apenas o que um indivíduo coloca dentro dele[36]".

[36] "[…] A compute is only what a person puts into it."

O perigo então é que a integração cada vez mais frequente da inteligência artificial nas atividades humanas, e consequentemente as jurídicas, pode ser tornar cada vez mais natural e inevitável, facilmente escondendo o caráter político das escolhas humanas que foram inevitavelmente adicionados a máquina (Simons, 2023. p. 31). Não há uma criação de vieses pela máquina, mas apenas um reflexo da realidade que já existe no sistema (Lowry, Macpherson, 1988, p. 657). O real problema não é referente a algum dado impreciso, mas de um dado que precisamente reflete um mundo de injustiça, sendo então os resultados obtidos por meio de Inteligência Artificial reveladores desigualdades sociais subjacentes (Simons, 2023. p. 23). Assim, a máquina pode terminar por ser uma mera extensão da injustiça social humana praticada.

Na busca de provas, isso reflete perigos relevantes, uma vez que a administração da justiça, da entrega de um processo equânime e do efetivo acesso aos direitos por um indivíduo, pode ficar comprometido. É exatamente o caso do Reino Unido anteriormente citado. No qual, após uma análise humana, foi constatado que 7.000 estudantes internacionais haviam sido falsamente acusados de terem burlado o teste de proficiência. E, por fim, o tribunal de recurso de imigração do Reino Unido concluiu que as provas utilizadas pelo Ministério do Interior para deportar os estudantes apresentavam múltiplas fragilidades e deficiências (Mcauliffe, 2021, p.6).

Dessa forma, todos os dados inseridos em uma máquina carecem de uma auditoria, mesmo que mínima, já que a equidade na IA depende da informação transmitida aos algoritmos. Em caso de uma informação minimamente tendenciosa, o resultado não será justo e a construção da prova já estará comprometida, não podendo ser entranhada ao processo. Bartneck (2021, p.37) explica que para que uma máquina seja confiável é necessário ter a certeza de que o sistema não trará malefícios ao indivíduo, que não comprometerá a sua autonomia, que o sistema pode atuar de forma justa dentro do seu âmbito funcional e que é explicável.

No que se refere a atuação justa, não há um referido consenso técnico, no sentido matemático, sobre como se daria essa aplicação para as máquinas, uma vez que o próprio conceito de equidade é subjetivo e tem ramificações diversas e nem sempre a matemática consegue abarcar todas essas possibilidades (Simons, 2023. p. 37-38). Além de que, os modelos de Inteligência Artificial de análise de dados podem ter diferentes formas, como preditivos, prescritivos, descritivos e analíticos (Kotsiopoulos, 2021, p. 2021), gerando formas totalmente diferente de gerar resultados, bem como de “implantar a equidade”.

Para exemplificar essa realidade, Josh Simons (2023, p. 36-54), analisando o caso do COMPASS, que se trata de um modelo preditivo, em sua pesquisa observou que a comunidade acadêmica para esse caso específico levantou pelo menos três teorias diferentes de aplicação de *fairness* (falso positivo e falso negativo, calibragem, anticlassificação, paridade demográfica) a uma máquina preditiva, as quais são até efetivas, mas não aplicáveis todas ao mesmo tempo e não são por si só garantias completas de uma total solução do problema por si só.

O autor relata que a ProPublica, site que denunciou o enviesamento do software, adotou o entendimento de que a equidade seria garantida quando as taxas de erros preditivos para pessoas brancas e negras fosse totalmente equivalente, ou seja que as porcentagens de falsos positivos e negativos fossem exatamente as mesmas independente da cor do indivíduo. Já a companhia que criou o COMPASS, a Northpoint, entendeu que a equidade da máquina dependeria de uma boa calibragem, seria garantida mediante a entrega de predições que signifiquem as mesmas coisas para os diferentes grupos sociais. Pontos, coerentes, mas que não poderiam ser aplicados juntos (Simons, 2023. p. 46).

A explicação do autor sobre essa questão é interessante e vale reproduzir:

> O resultado da impossibilidade é muito mais do que matemática. As definições de justiça da Northpointe e da ProPublica não podem ser alcançadas porque o resultado subjacente que o COMPAS procurava prever está distribuído de forma desigual entre negros e brancos. Este é um facto da sociedade, não da matemática, e requer o envolvimento com uma história complexa e marcada pelo racismo sistémico no sistema de justiça criminal dos EUA. Prever um resultado cuja distribuição é moldada por esta história requer compromissos, porque as desigualdades e injustiças do nosso mundo estão codificadas nos dados - neste caso, porque a América criminalizou a negritude desde que a América existe. O resultado não revela factos inexoráveis da matemática ou da natureza, mas sim algo sobre os compromissos envolvidos na previsão no contexto da desigualdade social. (Simons, 2023. p. 47-48)[37]

Então para além de uma solução matemática, que é coerente, é necessária uma análise profunda dos dados que serão introduzidos a máquina, das bases de dados utilizadas, dos parâmetros que serão estabelecidos e das informações que serão utilizadas como comparativos para que a máquina aprenda e chegue aos seus resultados. A equidade então depende de uma

[37] Tradução Livre de: "The impossibility result is about much more than math. Northpointe's and ProPublica's definitions of fairness cannot both be achieved because the underlying outcome that COMPAS sought to predict is distributed unevenly across Black and white people. This is a fact about society, not mathematics, and it requires engaging with a complex and checkered history of systemic racism in the US criminal justice system. Predicting an outcome whose distribution is shaped by this history requires trade-offs because the inequalities and injustices of our world are encoded in data-in this case, because America has criminalized Blackness for as long as America has existed. The result reveals not inexorable facts of mathematics or nature, but something about the trade-offs involved in prediction in the context of social inequality." (Simons, 2023. p. 47-48)

auditoria nos dados utilizados e dos vieses que podem introduzir e a partir disso direcionar as soluções matemáticas necessárias a cada caso.

5.1.2 Transparência (Transparency)

A transparência é o segundo princípio que deve ser levado em consideração, sendo bem definido como "a disponibilidade de informações sobre uma parte que permitam as outras partes controlar o seu funcionamento ou desempenho" (Bovens, Goodin, Schillemans, 2014, p.198). Trata-se exatamente da quantidade de informação disponível sobre uma determinada aplicação, que é suficiente para compreensão total do processo que envolve.

Gavighan (2019, p. 41) traz uma explicação relevante:

> [...] a transparência refere-se à responsabilidade, indicando uma resposta geral aos pedidos de informação ou uma vontade de oferecer uma justificação para as ações tomadas ou previstas. Neste sentido lato, a transparência é profiláctica - uma salvaguarda contra o abuso de poder. (Gavighan, 2019, p. 41)[38]

Dessa forma, transparência tem a ver com a prevenção de atividades arbitrárias por parte de quem detém controle sobre os resultados que a máquina produz. No caso da produção de provas digitais automatizadas o princípio da transparência apresenta-se como fundamental na garantia da lisura do processo de formação da prova, sendo fundamental para a entrega de uma cadeia de custódia segura.

No relatório final da Fase 1 do Projeto de Inteligência Artificial e Direito na Nova Zelândia da intitulado "*Government Use of Artificial Intelligence in New Zealand*"[39], há explicação de que a noção de transparência pode ser ramificada em pelo menos três direções específicas, tornando o conceito menos abstrato. A primeira seria a associação da transparência com à responsabilidade moral e legal, refletindo as noções comuns sobre culpa e responsabilidade por danos (Gavighan, 2019, p. 45). A exata entrega de informações coesas nos casos de situações sinistras, sobre a responsabilidade das partes envolvidas e esclarecimentos sobre as consequências que poderão se apresentar. Seria exatamente o direcionamento normativo das questões que envolvem o uso de Inteligência Artificial, apontamentos sobre

---

[38] Tradução Livre de: "[…] transparency refers to accountability, indicating a general responsiveness to requests for information or a willingness to offer justification for actions taken or contemplated. In this broad sense transparency is prophylactic—a safeguard against the abuse of power." (GAVIGHAN, 2019, p. 41)

[39] GAVIGHAN, Colin et al. Government use of artificial intelligence in New Zealand. **The New Zealand Law Foundation,** 2019.

quem responde pelos encargos financeiros que possam surgir e as medidas a serem tomadas em caso de danos e problemas.

A segunda direção seria exatamente o relacionamento da transparência com a inspecionabilidade (ou auditabilidade) das instituições, práticas e instrumentos. Seria a transparência em relação aos mecanismos utilizados, tanto no que se refere ao processo, como da técnica, que entraria também na noção da explicabilidade (Gavighan, 2019, p. 45). Nesse caso, a garantia de uma Inteligência Artificial transparente passa pela capacidade de responder perguntas como: Como é que este ou aquele instrumento funciona de fato? Como é que os seus componentes se articulam para produzir resultados como os que foram concebidos para produzir? Como foram desenvolvidos, por quem e com que objetivo(s)? Como é que ele funciona, com que dados foi treinado e segundo que lógica procede? A entrega dessas respostas permite aos indivíduos, que tem seus dados submetidos a uma aplicação inteligente, de alguma maneira a ter algum controle sobre seus direitos e ações a serem tomadas na defesa destes.

A terceira e última está relacionada a acessibilidade. Muitas vezes as explicações e respostas sobre um algoritmo podem ser até possíveis, mas podem não estar disponíveis, e a transparência passa também pela disponibilização e divulgação dessas respostas (Gavighan, 2019, p. 45). De nada adianta ser capaz de dar explicações sobre os códigos, os processos utilizados, se elas não estrão disponíveis ao público.

No contexto então da produção de provas digitais automatizadas esses três aspectos da transparência devem ser efetivamente levados em consideração. Uma vez que em casos de provas produzidas de forma ilegal ou com quaisquer tipos de vícios que geraram resultados desvantajosos, os indivíduos devem ser capazes de protestar por seus direitos e saber como o fazer e o que está ao seu alcance nesse sentido. Além disso, devem também ter respostas claras e explicações nítidas disponíveis sobre a forma que a máquina opera na produção da prova, compreendendo se os meios utilizados são seguros e efetivos, e, não sendo, tendo a possibilidade de impugnar de alguma maneira, preservando seus direitos.

Todos os casos apresentados no capítulo anterior requerem, em algum momento, alguma orientação em termos de transparência. No caso da atividade da Inteligência Artificial na busca por *Fake News*, é excepcional que a Justiça Eleitoral não apenas disponibilize informações sobre a aplicação, como também entregue explicações sobre o processo, como funciona, os dados analisados, como a máquina foi treinada, o responsável pelo projeto e

direcione normativamente as ações em caso de danos e arbitrariedades. Em relação a situação do Reino Unido seria interessante a disponibilização dos parâmetros utilizados para decidir se uma pessoa estava fraudando o teste ou não, dos dados inseridos no treinamento da máquina para que ela compreendesse o que seria uma fala proficiente em inglês, bem como o direcionamento sobre a possibilidade de impugnar a prova produzida pela da máquina e a quem responsabilizar em caso de erros.

No caso do COMPASS, seria imprescindível não apenas disponibilizar as informações técnicas sobre a máquina, mas também e principalmente a possibilidade de revisão e impugnação da prova que está sendo produzida e diretamente utilizada na decisão dos juízes. E, na Nova Zelândia, seria razoável, no início, o conhecimento da utilização da máquina para as predições realizadas que seriam base da tomada de decisão sobre os imigrantes.

Vale explicar, entretanto que a transparência caminha na linha divisória da necessidade real de entrega de informações sobre a existência de uma máquina e seu funcionamento e a importância da manutenção dos direitos de propriedade intelectual que impedem a divulgação de algumas informações técnicas, como o código, os dados de treino etc (GAVIGHAN, 2019, p. 45-46). Sobre isso, Blackman (2022, p. 36) explica que embora alguns exijam a máxima transparência máxima dos programas e códigos, quando se trata de sistemas de Inteligência Artificial isso pode não resolver um problema e pode até criar problemas. Nesse contexto há a seguinte exposição casuística:

> Suponha-se que um software com milhões de linhas de código é tornado transparente, qual seria a vantagem disso? Em primeiro lugar, o software não seria provavelmente inteligível para não especialistas e mesmo os especialistas e mesmo os especialistas teriam dificuldade em compreender o seu significado. Em segundo lugar, a transparência máxima do software poderia criar um risco em relação aos concorrentes e impedir novos investimentos neste setor. (Blackman, 2022, p. 36)[40]

Há, portanto, no contexto da transparência a necessidade de sopesar em que medida a rigidez na cristalinidade de informações técnicas é eficaz e garantidora de direitos para as partes que estão envolvidas no contexto da aplicação da máquina. Sendo esta inclusive uma das questões que mais preocupa os especialistas em políticas e um número crescente de cientistas da computação (Gavighan, 2019, p. 46). Especificamente, a esse tipo de consideração, algumas

[40] Tradução Livre de: "Suppose software containing millions of lines of code is made transparent, what would be the benefit of this? First, the software would probably not be intelligible to non-experts, and even experts would struggle with what it means. Second, maximal transparency of software might create a risk vis-a-vis competitors and hinder further investment in this sector. Due to considerations like these, some parts of the discussion have switched to the concept of "explicability". (Blackman, 2022, p. 36)

partes do debate passaram a utilizar o conceito de "explicabilidade" ou “inteligibilidade” (Blackman, 2022, p. 36). Que será analisada a seguir.

5.1.3 Explicabilidade (Explainability)

Como visto, as discussões sobre transparência inevitavelmente trazem a baila questões relativas a explicabilidade, já que não há efetiva transparência se não for possível entregar em alguma medida explicações coerentes e suficientes, para manutenção das garantias fundamentais, sobre a Inteligência Artificial aplicada. Floridi et al (2021, p. 30) sintetiza a explicabilidade em dois sentidos, um epistemológico, referente a “inteligibilidade” (como resposta a pergunta: Como isso funciona?), e outro ético, referente a “responsabilidade” (como resposta a seguinte pergunta: quem é o responsável pelo modo como funciona?).

Vale trazer à baila que em torno da explicabilidade existe uma grande zona cinzenta de dúvidas, que levanta questões como: Quem precisa saber como funciona? Que partes devem ser explicadas? E como a explicabilidade deve ser incorporada num processo intermediado por IA? (Montoya, Rummery, 2020, p.6). Levando em consideração essas questões e analisando o sentido epistemológico anteriormente apresentado, a explicabilidade se materializaria na compreensão precisa sobre como a Inteligência Artificial chegou a determinado resultado, por aqueles que utilizam sistemas de IA ou cujos interesses são afetados por esses sistemas (Floridi et al, 2021, p. 30), e continua:

> Inteligibilidade significa que o funcionamento da IA pode ser compreendido por um ser humano. O sistema não é uma "caixa negra" misteriosa cujo interior é ininteligível. Alguém, mesmo que seja apenas um programador experiente, pode compreender o funcionamento do sistema e explicá-lo aos juízes, júris e utilizadores. (Floridi et al, 2021, p. 30)

O princípio da explicabilidade então passa pela possibilidade de o sistema de IA ser compreendido por um ser humano, não necessariamente todos os indivíduos que de alguma forma tiverem contato com ele. Isso que dizer que algumas vezes a intelegibilidade só estará ao alcance de especialistas e não de leigos, entretanto, o que se espera, é que no caso de um eventual dano ou questionamento judicial sobre as condições técnicas de uma máquina, alguém seja capaz de explicar perante as autoridades judiciárias. O que compreende exatamente o segundo sentido da explicabilidade apresentado por Floridi et al (2021), a definição de um responsável por esclarecer o modo que a IA funciona, sendo capaz de oferece-las quando o for requerido, principalmente no contexto judicial.

Esse princípio não apenas permite a entrega efetiva do princípio da transparência, no sentido de permitir que informações sejam obtidas, como também e principalmente que se evite o uso de máquinas as quais nada se sabe sobre seu processo gerador de resultado. Haveria aqui um refreamento de submissão de indivíduos a softwares e programas os quais os resultados são inexplicáveis e de sem compreensão lógica.

Trata-se então de um dos princípios mais difíceis de aplicação prática, uma vez que não é tão fácil descobrir a razão completa pela qual a máquina chegou a determinados resultados, além do que pode envolver combinações, cruzamentos e inferências que combinadas que não são tão simples de explicar (Gavighan et al, 2019, p. 41). Como explica Bartneck (2021, p.42) essa é uma característica que distingue a Inteligência Artificial dos outros tipos de tecnologias, uma vez que podem operar de formas que são e certa forma, opacas para os observadores. Até mesmo para os próprios programadores, não possuem clareza sobre como exatamente o sistema chegou a esta ou àquela conclusão ou resultado. Não há sentido então na utilização de uma Inteligência Artificial com essas condições, é necessário um mínimo de entendimento sobre seus processos, uma vez que a falta desses esclarecimentos pode inclusive interferir na conformidade a outros princípios.

Esse princípio então se apresenta como complementar aos outros (Floridi et al, 2021, p. 30), tanto os que aqui apresentaremos especificamente, como aos que foram citados no início dessa seção como considerados por outros autores. Assim, para que a IA seja justa, há necessidade de compreender os dados nela inseridos para que ela realize os seus objetivos designados, bem como a razão de terem sido inseridos nas condições apresentados; para que esteja dentro dos padrões de responsabilidade e transparência deve-se de garantir que a tecnologia - ou, mais precisamente, as pessoas e organizações que a desenvolvem e implementam - seja responsabilizada no caso de um resultado negativo, o que exigiria, por sua vez, alguma compreensão da razão desse resultado; para seja considerada benéfica e não maléfica é necessário compreender o bem ou o mal que está efetivamente a fazer à sociedade, e de que forma (Floridi et al, 2021, p. 30).

Sendo esse trampolim para a efetiva aplicação dos outros e consequentemente para a manutenção da entrega justa dos direitos e garantias fundamentais dos indivíduos submetidos a aplicações de inteligência artificial, a explicabilidade deve ser formalmente estabelecida nas normativas. Devendo haver pelo menos um padrão de explicação que máquina deve dar, dependendo da situação, do objetivo do software e do tipo de IA utilizado.

5.1.4 Responsabilidade (Accountability)

De todos os princípios colocados, a responsabilidade é um dos únicos que é uma unanimidade quando analisados os documentos referentes a ética em Inteligência Artificial. Não se pode negar que os riscos no uso da IA são eminentes e precisam ser reparados por algum agente, seja este o desenvolvedor ou o aplicador da máquina em determinado contexto. Assim, a aplicação do princípio da responsabilidade passa necessariamente pela definição de uma responsável por arcar com os ônus requeridos em caso de qualquer acidente envolvendo um robô ou um sistema de IA (Bartneck, 2021, p.39). Trata-se de um desafio, devido à complexidade da maioria dos casos (como o da migração no Reino Unido) e à complexidade do próprio sistema.

A responsabilidade é um princípio que é inevitavelmente requerido pelos outros princípios. Como podemos recordar, a transparência em uma das três direções que pode tomar, uma delas refere-se necessariamente ao direcionamento translucido dos responsáveis em caso de danos e ocorrências juridicamente desastrosas, bem como das ações que podem ser tomadas pelos afetados. Já na explicabilidade, em um dos dois sentidos que aplicação há necessidade de se definir o responsável por dar explicações sobre a máquina e seus processos, sendo o indivíduo que deverá se apresentar juridicamente a trazer informações que ajudarão a definir o grau de responsabilidade dos agentes e suas intenções com o uso da aplicação.

A responsabilidade pode apresentar várias ramificações a depender do caso analisado, pode se apresentar com objetiva, subjetiva, pode gerar responsabilização por ricochete, dentre outros desdobramentos. Ademais, as aplicações e interpretações relativas a responsabilidade podem varias a depender da situação em que a Inteligência Artificial é aplicada e seu tipo. Por exemplo, já há ampla discussão acadêmica, bem como direcionamentos normativos em alguns países, sobre a responsabilidade em caso de batidas causadas por carros autônomos.

A intenção desse trabalho, entretanto, não é esgotar todas as possibilidades que esse princípio apresenta, uma vez que seria inviável. Direcionando, então, a aplicação do princípio da responsabilidade especificamente para o contexto jurídico probatório, em que a aplicação da inteligência artificial nesse contexto será aplicada ou pelo estado, em contexto de investigação e perícia, ou em casos específicos pelo réu, mediante explícita autorização do juízo para o entranhamento das provas obtidas, esse será o foco abordado. Vale ressaltar também, que em razão da atualidade da pesquisa aqui proposta, não há pesquisas, doutrinas e discussões específicas sobre responsabilidade ao uso de IA na produção probatória digital, assim

adotaremos uma análise por aproximação, de forma que finalmente haja um mínimo direcionamento por onde a responsabilização nesse caso deve seguir.

No que se refere a aplicação Estatal e Governamental de inteligência artificial na condução de investigação probatória, de perícia digital etc, é possível inferir que a responsabilidade recairá sobre o órgão público, utilizando o conceito de responsabilidade objetiva, na qual "não se exige prova de culpa do agente para que seja obrigado a reparar o dano" (Gonçalves, 2023, p. 25), sendo prescindível, pois se fundamenta no risco. Barneck et al (2021, p.42) explicam que no caso da responsabilidade objetiva, pode nem sequer ter havido uma infração concreta, podendo a empresa, o órgão ou pessoa ser responsabilizado mesmo que não tenha diretamente feito nada de errado em sentido estrito. Como no caso de alguém que possui um cão ou um gato e o animal causa danos à propriedade de outra pessoa, o proprietário é considerado responsável neste sentido.

Nessa perspectiva, uma vez que o órgão público decide por aplicar a Inteligência Artificial para realização de determinada produção de prova, para fundamentação de algum tipo de decisão ou administração de serviço, assume-se o risco administrativo sobre quaisquer danos que vier a gerar no cidadão que diante de alguma condição foi submetido ao sistema. O caso, do Reino Unido, citado anteriormente, ilustra bem essa questão, pois é claro que o Estado estava dependente dos resultados de uma terceira empresa para tomar a sua decisão, mas como se tratava de uma atividade do governo (imigração) e provinha do departamento público o resultado final, a responsabilidade então é do órgão governamental migratório. O ente estatal então deve ter como certo que a aplicação de IA em suas atividades ensejará sua responsabilidade.

No que se refere a produção probatória digital automatizada viabilizada pelo réu, na pessoa de seus advogados, ou representantes jurídicos, mesmo que autorizada juridicamente, já se aplica de outra maneira. Nessa situação específica, trazemos a baila a comparação com a responsabilidade civil do administrador de sociedades empresárias, que é subjetiva (Medon, 2022, p. 399). Há necessidade do agente, que irá escolher a aplicação de IA que irá submeter a sua produção probatória, para juntar ao processo, munir-se do dever de diligência, uma vez que ele é responsável por analisar o risco da utilização do sistema escolhido (Frazão, 2019, p. 506). Nesse caso, então, tendo o réu confiado aos seus advogados a sua causa, bem como a decisão de como realizar a produção probatória, uma vez comprovada a culpa advocatícia na falta de cuidado na busca de um sistema automatizado para produção de provas, estes serão

responsabilizados ao dano que causarem ao cliente. É inequívoco que se trata de um exercício desafiador, já que há muitos sistemas que não são transparentes, de forma que nem sempre é possível saber como a máquina opera, entretanto, apesar dessa dificuldade é premissa certa de que não se pode ter uma confiança cega no sistema de Inteligência Artificial (Frazão, 2019, p. 506).

De outra forma, comprovada a lisura, dos advogados, pode-se buscar a responsabilidade nos desenvolvedores do sistema de IA. Novamente, trata-se de uma responsabilidade subjetiva, já que nesta apuração "será preciso averiguar a diligência empregada pelos sujeitos que participaram da programação algorítmica" (Medon, 2022, p. 411). Nesses casos, pode ser difícil apontar um agente responsável, já que frequentemente as ferramentas de IA possuem um desenvolvimento difuso, tendo múltiplos agentes que contribuíram para formação do sistema (Scherer, 2015, p. 370), o que pode dificultar substancialmente o direcionamento definitivo de quem irá arcar com os ônus ensejados.

É nesse contexto, que Frazão (2021, p.35) apresenta a possibilidade de se definir uma cadeia de responsabilidade pelas consequências do emprego da tecnologia, sendo uma nova realidade a ser considerada pelo direito. Isso, porque como a inteligência artificial é uma tecnologia facilmente distribuída e difundida, sem a necessidade de grande investimento em infraestrutura, a responsabilidade também não precisa necessariamente estar concentrada nas mãos de um único agente (Frazão, 2021, p.35). Sendo está uma solução célere para a entrega de uma solução ou reparação para o indivíduo prejudicado.

Por fim, vale pontuar a análise de Jacob Turner (2018, p. 91) referente a realidade da imprevisibilidade das ações da Inteligência Artificial, em que não se tem como prever com segurança que o resultado encontrado será exatamente o que se pretende. Tal é capaz de mudar o foco da atribuição dessa responsabilidade aos humanos por todas as ações de uma IA, passando a estar "menos ligada à culpa do agente humano e mais a um sistema de responsabilidade objetiva ou pelo fato do produto" (Medon, 2022, p. 415). Essa autonomia da máquina ainda enseja a possibilidade do desenvolvimento de uma personalidade a robôs (Medon, 2022, p. 415), o que entrariam em discussões mais profundas que aqui não cabem especificamente.

Do exposto, o que se obtêm é que a responsabilidade deve estar definida. Não haverá como entregar um devido processo legal, permitindo a produção probatória de provas por

inteligência artificial, se esse sistema não apresentar nenhum mecanismo de atendimento a responsabilidades civil em caso de danos. Novamente, se assim, for a prova não será admissível e será tida como ilegal, não podendo ser utilizada.

5.2 Admissibilidade normativa na produção da prova digital

O despontamento de novas tecnologias resulta inevitavelmente em consequências para o direito e a justiça, uma vez que a organização jurisdicional reflete diretamente as características culturais, econômicas, políticas e culturais de uma sociedade. Assim, "se a sociedade passa a enfrentar uma eclosão de novas tecnologias de informação, é infestável seu reverbério nos campos do direito [...]" (Souza, 2021, p.13), uma vez que a pressão para que as normas sejam atinentes a realidade imposta será sentida.

É exatamente sob essa perspectiva que se assenta a necessidade de regulamentação normativa do uso de Inteligência Artificial na produção probatória, uma vez que os desafios são significativos e representam consequências imediatas aos direitos dos indivíduos. Entretanto, há ainda "pouquíssimas leis ou regulamentações que tratam especificamente dos desafios trazidos pela inteligência artificial" (Lage, 2021, p. 160). O que tem gerado uma falta de alinhamento entre a realidade avançada do desenvolvimento da tecnologia e suas consequências em contraste com a entrega jurisdicional de soluções apropriadas.

Sobre essa realidade Schwab (2019, p. 21) sinaliza dois pontos de preocupação:

> Primeiro, acredito que os níveis exigidos de liderança e compreensão sobre as mudanças em curso, em todos os setores, são baixos quando contrastados com a necessidade, em resposta à quarta revolução industrial, de repensar nossos sistemas econômicos, sociais e políticos. O resultado disso é que, nacional e globalmente, o quadro institucional necessário para governar a difusão das inovações e atenuar as rupturas é, na melhor das hipóteses, inadequado e, na pior, totalmente ausente. Em segundo lugar, o mundo carece de uma narrativa coerente, positiva e comum que descreva as oportunidades e os desafios da quarta revolução industrial, uma narrativa essencial caso queiramos empoderar um grupo diversificado de indivíduos e comunidades e evitar uma reação popular contra as mudanças fundamentais em curso. (grifo nosso)

Há então um problema evidente de acompanhamento síncrono do direito a realidade de desenvolvimento, o que inevitavelmente pode gerar uma barreira a continuidade da inovação e do despontamento de novas tecnologias computacionais. Não é coerente, portanto, manter essa realidade, Caletti e Staffen (2019, p. 282) explicam que o direito inevitavelmente precisa se amoldar às manifestações sociais do momento histórico, rompendo com as antigas metodologias distinguindo-se as questões pretéritas daquelas presentes (Vaz, 2012).

Por outro lado, quando se trata de Inteligência Artificial, apesar da amplitude de sua influência e seu alastramento progressivo, as consequências jurídicas não são totalmente conhecidas (Rincon-Salcedo, 2015), o que gera um impasse: além da necessidade inegável de regular, não se sabe todas as situações que deverão ser abarcadas. Sobre isso, Lage (2021, p. 161) explica que é fundamental compreender o que a regulamentação pode ou não pode fazer, para que então se possa pensar adequadamente a normatização, de forma que seja exequível não apenas para os que produzem a tecnologia, como para os que usam, sem, entretanto, reprimir os avanços científicos.

Essa regulamentação então possui peculiaridades intrínsecas que devem ser consideradas no processo de desenvolvimento normativo, para que então tenham resultado eficazes, ou seja, sejam aceitas como legítimas e institucionalizadas, em oposição a regras meramente formais ou simbólicas (Erdélyi; Goldsmith, 2018, p. 96). Ademais, embora as normas jurídicas tenham suas raízes predominantemente sociais e não morais, as considerações éticas devem e irão desempenhar um papel relevante na formação da normativa nascente no que se refere a inteligência artificial (Erdélyi; Goldsmith, 2018, p. 96). Dessa forma, quando se fala em normativa referente a Inteligência Artificial, deve ser levado em consideração as questões sociais que suscita e com ela as questões éticas que a envolvem. Então os princípios éticos assinalados anteriormente, necessariamente deve fazer parte das predições normativas.

Quando se fala de regulamentação normativa de inteligência artificial, em qualquer setor que seja inserida, há pelo menos duas questões paradoxais que se levantam: a primeira é que uma boa regulação seria capaz de mitigar novos riscos que o uso de inteligência artificial cria, a segunda é que os riscos de uma má regulação são capazes de refrear o desenvolvimento e entrega de soluções relevantes que essa ferramenta proporciona (Reed, 2018, p. 2). Nessa perspectiva Scherer (2016) traz à tona dois panoramas possíveis ligados a regulamentação de Inteligência Artificial, o primeiro seria o desenvolvimento de normativas após a máquina causar danos, o que é problemático, uma vez que não haveria minimização de riscos. O segundo seria o desenvolvimento normativo antes do desenvolvimento da máquina, o que também é complicado, pois não se pode ter certeza do que pode vir com o desenvolvimento da IA ao longo dos anos.

Entretanto, compreendendo que não se pode dar as costas para a realidade de desenvolvimento e inovação que se alastra, são necessárias movimentações normativas, mesmo

que sejam em formas de diretivas, padrões mínimos ou documentos de boas práticas, para que então posteriormente sejam promulgadas normativas mais específicas.

Como explicado, desde o início dessa pesquisa, há consciência de que não existem muitos trabalhos, pesquisas e normativas que falam diretamente desse conceito de prova que aqui foi apresentado. Mas sabendo da realidade de sua aplicação, buscamos encontrar nas normativas disponíveis atualmente que possam minimamente direcionar ou prever a acolhida desse tipo de prova, bem como normativas em vias de desenvolvimento que possam vir a auxiliar nesse contexto.

A primeira normativa analisada é a Resolução Nº 332 de 21/08/2020 do Conselho Nacional de Justiça - CNJ, o qual traz direcionamentos relevantes no que diz respeito a aplicação de Inteligência Artificial no contexto do judiciário. Já em seu artigo 2° dispões que que a IA no âmbito do poder judiciário, tem como finalidade não somente promover a bem-estar dos jurisdicionados e a prestação equitativa da jurisdição, mas também "descobrir métodos e práticas que possibilitem a consecução desses objetivos". Considerando que a utilização da prova digital automatizada auxilia significativamente no esclarecimento de fatos, que de outra forma não teriam soluções tão intuitivas, permitindo o acesso aos direitos, bem como a celeridade nessa prestação.

A normativa ainda apresenta disposições que abarcam o respeito aos princípios da justiça (Artigos 4°, 5°, 6°, 13°, 14°, 15° e 16°), Transparência (Artigo 8°), Explicabilidade (Artigo 17°, 18° e 19°) e Responsabilidade (Artigos 25°, 26° e 27°), bem como preveem o combate a aplicação de máquinas enviesadas (Artigo 7°).

Há, entretanto, no Artigo 23° uma disposição que pode ser impeditiva ao uso das provas digitais automatizadas uma vez que esse dispõe que não se deve estimular a utilização de modelos de Inteligência Artificial em matéria penal. Tal fato, se configura como dificultador, uma vez que o processo penal seria onde mais haveria aplicações, já que é onde normalmente são necessárias buscas de provas com mais afinco, além de ser a matéria que mais possui normativas direcionadoras no que se refere a provas.

Um outro documento importante é o Projeto de Lei 2.338, de 2023, do Senado Federal, que está ainda em tramitação em vias de aprovação. O interessante desse texto é que em seu artigo 17°, onde classifica as IAs de alto risco, inclui em sua lista aquelas que tem como finalidade de:

> [...] investigação por autoridades administrativas para avaliar a credibilidade dos elementos de prova no decurso da investigação ou repressão de infrações, para prever a ocorrência ou a recorrência de uma infração real ou potencial com base na definição de perfis de pessoas singulares.

Aqui é possível perceber uma previsão mais direta a prova digital automatizada, mas sendo classificada como um sistema de alto risco o qual deverá passar por uma análise árdua de suas condições de aplicação, além do sopesamento dos riscos que pode gerar, bem como o exame de sua submissão aos critérios éticos impostos (a saber: transparência, explicabilidade e auditabilidade).

Um último documento relevante é o Projeto de Lei 4.939/2020, que dispõe sobre as diretrizes do direito da Tecnologia da Informação e as normas de obtenção e admissibilidade de provas digitais na investigação e no processo, sendo então uma normativa mais específica a provas digitais. Nesse documento, no artigo 5° há a seguinte disposição:

> Art. 5º A admissibilidade da prova nato-digital ou digitalizada na investigação e no processo exigirá a disponibilidade dos metadados e a descrição dos procedimentos de custódia e tratamento suficientes para a verificação da sua autenticidade e integridade. Parágrafo Único: Caso a prova digital seja produto de tratamento de dados por aplicação de operação matemática ou estatística, de modo automatizado ou não, devem estar transparentes os parâmetros e métodos empregados, de modo a ser possível a sua repetição e reprodutibilidade. (grifo do autor)

Uma disposição já mais promissora no que se refere as provas digitais automatizadas, uma vez que está prevista a sua possibilidade, desde que esteja submetida aos procedimentos de custódia e disponibilização dos dados utilizados (princípio da transparência e da justiça). Apesar de demonstrar perspectivas promissoras, o Projeto ainda não foi aprovado e não previsão para que isso ocorra. O que demonstra que apesar das boas intenções em atender uma necessidade real, não há o devido impulso para que ocorra com mais celeridade.

6 CONCLUSÃO

A prova digital automatizada não é uma realidade distante da vida jurídica, mesmo com poucas doutrinas, pesquisas e normativas nesse sentido, as aplicações sociais já se fazem presente e já tem sido incluída em alguns casos. Não há mais como retroceder no que se refere a inserção da tecnologia nas questões sociais e jurídicas, daqui em diante é necessária uma movimentação no sentindo da produção normativa e da submissão aos padrões éticos.

Antes, entretanto, de se chegar a esse ponto, é necessária analisar toda a base do que a prova digital automatizada seria composta, de forma a sustentar sua relevância e efetiva introdução ao processo judicial. Inicialmente, é fundamental recordar que o direito a prova é um direito constitucional, sendo meio garantidor da dignidade humana, na concretização de um devido processo legal e o consequente acesso aos seus direitos. Por isso, deve ser preservado, sendo capaz de habilitar a inclusão de diversos meios probatórios aptos a concretização do direito a prova, bem como relevantes ao processo.

É fundamental compreender, entretanto, que não são todas as evidências encontradas no contexto digital que podem ser efetivamente utilizadas como provas em um processo. Para que sejam consideradas provas válidas, as evidências deverão ser consideradas aptas e isso depende da conformidade aos requisitos materiais e formais. Assim, as evidências devem ser normativamente previstas e não violar princípios e direitos constitucionais, atendendo seguramente a esses quesitos, mesmo que não sejam modalidades típicas, não podem ser impedidas de integrar o processo.

A prova digital, então, aparece como um tipo de prova plausível de inclusão no processo judicial. Entretanto, sua admissibilidade merece atenção, já que mesmo sendo prevista de forma tímida nas normativas, ainda é considerada como opção excepcional de prova, além de não ter uma cadeia de custódia bem definida, o que pode impedir a concretização de sua fiabilidade dentro do processo.

Vale ressaltar que o Brasil, apesar da instituição da Cadeia de Custódia da prova em seu pacote anticrime, este se refere mais a obtenção de provas físicas, não contemplado a totalidade das características e particularidades da prova digital. O que é um ponto de atenção relevante.

Ocorre que, apesar dessa realidade ainda pendente de algumas respostas e soluções no que se refere a prova digital, a dispersão tecnológica nas relações jurídico-sociais continua. A Inteligência Artificial segue avançando em seu desenvolvimento e alcançando cada vez mais setores da comunidade, inclusive o processo judicial. Mediante os casos citados, é possível perceber que não se trata apenas de uma realidade próxima, mas também de aplicações diversas abarcando ambas as partes de um processo.

Essa inserção da Inteligência Artificial na produção probatória gera uma significativa celeridade na condução probatória e consequentemente na condução do processo como um todo, de diminuir os custos que de outra forma seriam elevados, além de permitir encontrar soluções que de outra forma não seriam encontradas ou dependeriam de uma série de fases para isso. Por outro lado, há a realidade de que a Inteligência Artificial não é uma aplicação totalmente madura e nem mesmo chegou-se ao entendimento completo do que ela é capaz, o que pode gerar resultados imprevisíveis que frequentemente podem afetar diretamente as garantias fundamentais de um indivíduo.

Dessa forma, para que seja admissível em um processo judicial a prova digital automatizada deve inicialmente submeter-se a uma admissibilidade normativa, sendo prevista por meio de leis, diretivas, mecanismos de boas práticas etc., bem como a uma admissibilidade ética, uma vez que aplicações que envolvem a aplicação de inteligência artificial precisam garantidamente (mesmo que de forma mínima) justas, transparentes, explicáveis e passíveis de responsabilização.

Mediante toda a análise feita, é possível perceber que o Brasil ainda precisa de melhores direcionamentos tanto no que se refere a normatização de provas digitais, quanto ao uso de Inteligência Artificial. Apenas mediante a aplicação das normativas internas não será possível permitir facilmente a utilização de provas digitais automatizadas ao processo judicial, uma vez que são poucas e muitas ainda nem forma efetivamente promulgadas, apesar de já serem fomentadoras de diversas discussões sobre esse tema no país.

Tal fato representa um grande impasse, uma vez que representa um desestimulo a inovação e uso de aplicações tecnológicas no contexto jurisdicional, além de impedir a aplicação alternativa de um direito constitucional que é a prova, já que se vive em uma comunidade digital e boa parte das relações com desdobramentos jurídicos acontecem dentro desse ambiente.

Para isso então é necessário que o Brasil desenvolva uma normativa que preveja a cadeia de custódia da prova digital, sendo o este o tema para um trabalho futuro, incluindo nesta a possibilidade de aplicação de inteligência artificial, bem como desenvolva com mais celeridade normativas concernentes ao uso de inteligência artificial no contexto judicial e processual, direcionando os aspectos éticos e medidas preventivas de riscos.

REFERÊNCIAS

ADAM, Iliyasu Yahaya; VAROL, Cihan. Intelligence in digital forensics process. In: 2020 8th **International Symposium on Digital Forensics and Security (ISDFS)**. IEEE, 2020. p. 1-6.

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.

ALMEIDA, Ivo Filipe de. **A prova digital.** 2015. Dissertação (Mestrado em Ciências Jurídicas) – Departamento de Direito, Universidade Autónoma de Lisboa, Lisboa, Portugal, 2015. Disponível em: https://repositorio.ual.pt/bitstream/11144/1849/1/A%20prova%20Digital%20%28Disserta%C3%A7%C3%A3o%29%20%281%29.pdf. Acesso em: 30 set 2023.

BARRETO, Alesandro Gonçalves; WENDT, Emerson. **Inteligência e Investigação Criminal em Fontes Abertas**. Brasport, 2020.

BARTNECK, Christoph et al. **An introduction to ethics in robotics and AI**. Springer Nature, 2021.

BARTNECK, Christoph et al. An introduction to ethics in robotics and AI. **Springer Nature**, 2021.

BARZOTTO, Luciane Cardoso. A Prova Digital como Meio de Prova Atípica: Aspectos Teóricos e um Caso Prático. In: MISKULIN, Ana Paula Silva Campos; BERTACHINI, Danielle; NETO, Platon Teixeira de Azevedo (org.). Provas Digitais no Processo do Trabalho: Realidade e Futuro. Campinas, São Paulo: Lacier Editora, 2022. P. 95-106

BASSIL, Youssef. A Digital Forensics Framework for Facebook Activity Logs**. IOSR Journal of Computer Engineering (IOSR-JCE)**, v. 21, p.12-18, 2019.

BLACKMAN, Reid. Ethical machines: your concise guide to totally unbiased, transparent, and respectful AI. **Harvard Business Review Press.** 2022.

BOVENS, Mark; GOODIN, Robert E.; SCHILLEMANS, Thomas (Ed.). **The Oxford handbook public accountability**. Oxford University Press, 2014.

BRASIL. Superior Tribunal de Justiça (6. Turma). Agravo Regimental no Habeas Corpus 803.700– RS. Agravo regimental no habeas corpus. Associação para o tráfico de drogas. Excesso de prazo. Supressão de instância e prejudicialidade. Quebra da cadeia de custódia. Nulidade não constatada. Prisão preventiva. Fundamentação válida. Ausência de ilegalidade. Agravante: Gabriel Robeck. Agravado: Ministério Público Federal e Ministério Público do Estado do Rio Grande do Sul. Impetrado: Tribunal de Justiça do Estado do Rio Grande do Sul. Relator: Min. Jesuíno Rissato (Desembargador Convocado do TJDFT), 28 de agosto de 2023. Diário de Justiça Eletrônico, 30 ago. 2023. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202300513099&dt_publicacao=30/08/2023. Acesso em 09 dez 2023.

BRASIL. Superior Tribunal de Justiça. Habeas Corpus 435.813– SP. Impetrante: Luiz Antonio Zuliani. Impetrado: Tribunal Regional Federal da 3ª Região. Relator: Min. Rogerio Schietti Cruz, 07 de fevereiro de 2018. Diário de Justiça Eletrônico, 8 fev. 2018. Disponível em: https://processo.stj.jus.br/processo/monocraticas/decisoes/?num_registro=201800259473&dt_publicacao=09/02/2018. Acesso em 09 dez 2023.

BRASIL. Supremo Tribunal Federal (2. Turma). Agravo Regimental no Habeas Corpus 171.557 – PR. Agravo Regimental No Habeas Corpus. Processo Penal. ART. 22 da lei n. 7.492/1986. Alegação de quebra da cadeia de custódia das provas e ilicitude probatória. Impossibilidade de reexame do quadro fático-probatório na via eleita. Precedentes. Agravo regimental ao qual se nega provimento. Agravante: Hussain Said Mourad. Agravado: Superior Tribunal de Justiça. Relator: Min. Cármen Lúcia, 18 de outubro de 2023. Diário de Justiça Eletrônico, 1 dez. 2023.Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=773144078. Acesso em 09 dez 2023.

BREZINSKI, D.; KILLALEA, T. Guidelines for Evidence Collection and Archiving. IETF. Online, 2002. Disponível em: https://www.ietf.org/rfc/rfc3227.txt Acesso em: 04 dez 2023.

CALETTI, Leandro; STAFFEN, Márcio Ricardo. A fragmentação jurídica e o direito ambiental global. **Veredas do Direito: Direito Ambiental e Desenvolvimento Sustentável**, v. 16, n. 34, p. 279-310, 2019.

Capanema, Walter Aranha. **Manual de Direito Digital**: teoria e prática. São Paulo: Editora JusPodivm, 2024.

CARRIER, Brian D. et al. Automated Digital Evidence Target Definition Using Outlier Analysis and Existing Evidence. In: **DFRWS**. 2005.

CARRIER, Brian. **A hypothesis-based approach to digital forensic investigations**.CERIAS Tech Report, 2006.

CASEY, Eoghan. **Digital evidence and computer crime: Forensic science, computers, and the internet.** Academic press, 2011.

CHORAŚ, Michał et al. Machine Learning–the results are not the only thing that matters! What about security, explainability and fairness?. **In: Computational Science–ICCS 2020: 20th International Conference, Amsterdam, The Netherlands, June 3–5, 2020, Proceedings, Part IV 20. Springer International Publishing**, 2020. p. 615-628.

CHRISTIAN, Brian. **The alignment problem: How can machines learn human values?**. Atlantic Books, 2021.

ĆOSIĆ, Jasmin; ĆOSIĆ, Zoran; BAČA, Miroslav. An ontological approach to study and manage digital chain of custody of digital evidence**. Journal of Information and Organizational Sciences**, v. 35, n. 1, p. 1-13, 2011.

DORLEON, Ginel. **Mitigation of Data Bias through Fair Features Selection Methods**. 2023. Tese de Doutorado. Paul Sabatier. Université Toulouse III-Paul Sabatier (UPS), Toulouse, FRA.

DUHIGG, Charles. How companies learn your secrets. In: The Best Business Writing 2013. Columbia University Press, 2013. Disponível em: http://www.nytimes.com/2012/02/19/magazine/shoppinghabits.html?pagewanted=1&_r=1&hp. Acesso em: 22 ago. 2023.

DUNSIN, Dipo et al. The use of artificial intelligence in digital forensics and incident response in a constrained environment. **International Journal of Information and Communication Engineering**, v. 16, n. 8, p. 280-285, 2022.

ERDÉLYI, Olivia J.; GOLDSMITH, Judy. Regulating artificial intelligence: Proposal for a global solution. **In: Proceedings of the 2018 AAAI/ACM Conference on AI, Ethics, and Society.** p. 95-101. 2018.

FENOLL, Jordi Nieva et al. **Inteligencia artificial y proceso judicial**. Madrid: Marcial Pons, 2018.

FLORIDI, Luciano et al. An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. **Ethics, governance, and policies in artificial intelligence**, p. 19-39, 2021.

FORD, Martin. **Rule of the robots: How artificial intelligence will transform everything**. Hachette UK, 2021.

FRAZÃO, Ana. Responsabilidade civil de administradores de sociedades empresárias por decisões tomadas com base em sistemas de inteligência artificial. **Inteligência artificial e direito: ética, regulação e responsabilidade. Editora Revista dos Tribunais**, 2019.

FRAZÃO, Ana; GOETTENAUER, Carlos. Black box e o direito face à opacidade algorítmica. **Barbosa, Mafalda Miranda. Direito Digital e Inteligência Artificial. Indaiatuba: Editora Foco**,v. 79, 2021.

GAROFALO NETO, Emílio. Isto é Filtro Solar. Brasília, DF: Editora Monergismo, 2020.

GAVIGHAN, Colin et al. Government use of artificial intelligence in New Zealand. **The New Zealand Law Foundation**, 2019.

GIOVA, Giuliano et al. Improving chain of custody in forensic investigation of electronic digital systems. **International Journal of Computer Science and Network Security**, v. 11, n. 1, p. 1-9, 2011.

GONÇALVES, Carlos R. **Responsabilidade Civil**. Editora Saraiva, 2023. E-book. ISBN 9786553624450. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786553624450/. Acesso em: 21 jan. 2024.

HINTZ, Arne; DENCIK, Lina; WAHL-JORGENSEN, Karin. **Digital citizenship in a datafied society**. John Wiley & Sons, 2018.

HLEG, A. I. Ethics Guidelines for Trustworthy Artificial Intelligence. **High-Level Expert Group on Artificial Intelligence**, v. 8, 2019.

International Organization for Standardization (ISO), **ISO/IEC 27037:2012 - Information Technology: Guidelines for Identification Collection Acquisition and Preservation of Digital Evidence**. 2012.

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

ISO/IEC 27037. Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 27037:2012 - Tecnologia da informação - Técnicas de segurança: Diretrizes para identificação, coleta, aquisição e preservação de evidência digital. 2013.

JARRETT, Aaron; CHOO, Kim-Kwang Raymond. The impact of automation and artificial intelligence on digital forensics. **Wiley Interdisciplinary Reviews: Forensic Science**, v. 3, n. 6, p. e1418, 2021.

JOBIN, Anna; IENCA, Marcello; VAYENA, Effy. The global landscape of AI ethics guidelines. **Nature machine intelligence**, v. 1, n. 9, p. 389-399, 2019.

KIST, Dario José. **Prova digital no processo penal**. Leme: JH Mizuno, 2019.

KOTSIOPOULOS, Thanasis et al. Machine learning and deep learning in smart manufacturing: The smart grid paradigm. **Computer Science Review**, v. 40, p. 100341, 2021.

KUZIEMSKI, Maciej; MISURACA, Gianluca. AI governance in the public sector: Three tales from the frontiers of automated decision-making in democratic settings. **Telecommunications policy**, v. 44, n. 6, p. 101976, 2020.

LAGE, Fernanda de Carvalho. Manual de inteligência artificial no direito brasileiro**. Salvador: JusPodivm**, 2021.

LANGFORD, Malcolm. Taming the digital leviathan: Automated decision-making and international human rights. **American Journal of International Law**, v. 114, p. 141-146, 2020.

LARONGA, Antonio. Le prove atipiche nel processo penale. Padova: Cedam, 2002.

LIMA, Renato Brasileiro de. **Pacote Anticrime**: Comentários à Lei 13.964/2019 artigo por artigo. Salvador: JusPodivm, 2020.

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

LOWRY, Stella; MACPHERSON, Gordon. A blot on the profession. **British medical journal (Clinical research ed.)**, v. 296, n. 6623, p. 657, 1988.

MAIER, Julio BJ. **Derecho procesal penal**. Buenos Aires: Editores Del Puerto, 2011.

MARINONI, Luiz Guilherme; ARENHART, Sérgio Cruz. Prova e convicção. 5. ed. São Paulo: **Thomson Reuters**, 2019.

MARMELSTEIN, George**. Curso de Direitos Fundamentais**. São Paulo: Atlas, 2019.

MASSENA, Caio Badaró. Inteligência Artificial e prova penal. **Trincheira Democrática – Boletim Revista do Instituto Baiano de Direito Processual Penal**, ano 2, n.6, Salvador, IBADPP, p. 28-32, dezembro de 2019.

MCAULIFFE, Marie. International migration and digital technology: an overview. **Research handbook on international migration and digital technology**, p. 1-13, 2021.

MEDON, Filipe. Inteligência Artificial e responsabilidade civil. **Salvador: Juspodivm**. 2022.

MEIRELES, Ana Isa Dias**. A prova digital no processo judicial**. Coimbra: Almedina, 2023.

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

MITCHELL, Faye. The use of Artificial Intelligence in digital forensics: An introduction. **Digital Evidence & Elec. Signature L. Rev**., v. 7, p. 35, 2010.

MONTEIRO, João. **Programma do curso de processo civil**. v. 2., 3. ed. São Paulo: Duprat, 1912.

MONTOYA, Daniel; RUMMERY, Alice. The use of artificial intelligence by government: parliamentary and legal issues. **NSW Parliamentary Research Service**. 2020.

MORAIS, Jose Luis Bolzan de. Missão de observação eleitoral: o controle, pela justiça eleitoral, do uso e impacto das redes sociais no processo eleitoral: relatório final. 2023. Disponível em: https://www.tse.jus.br/++theme++justica_eleitoral/pdfjs/web/viewer.html?file=https://www.tse.jus.br/eleicoes/eleicoes-2022/arquivos/missoes-de-observacao-eleitoral-nacionais/faculdade-de-direito-de-vitoria-ppgd-fdv/@@download/file/TSE-faculdade-de-direito-de-vitoria-ppgd-fdv.pdf. Acesso em: 07 Jan 2024.

NERES, Winícius Ferraz. A cadeia de custódia dos vestígios digitais sob a ótica da Lei n. 13.964/2019: aspectos teóricos e práticos. **Boletim Científico ESMPU**, Brasília, ano 20, n. 56, jan./jun., 2021. Disponível em: https://escola.mpu.mp.br/publicacoes/boletim-cientifico/edicoes-do-boletim/boletim-cientifico-n-56-janeiro-junho-2021/a-cadeia-de-custodia-dos-vestigios-digitais-sob-a-otica-da-lei-n-13-964-2019-aspectos-teoricos-e-praticos. Acesso em: 23 jan. 2024.

NISSAN, Ephraim. Digital technologies and artificial intelligence's present and foreseeable impact on lawyering, judging, policing and law enforcement. **Ai & Society**, v. 32, p. 441-464, 2017.

NISSAN, Ephraim. Legal evidence, police intelligence, crime analysis or detection, forensic testing, and argumentation: an overview of computer tools or techniques. **International Journal of Law and Information Technology**, v. 17, n. 1, p. 1-82, 2009.

OMEZI, Natasha; JAHANKHANI, Hamid. Proposed forensic guidelines for the investigation of fake news. **Policing in the Era of AI and Smart Societies**, p. 231-265, 2020.

Paulo, 2006.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.

PINHEIRO, Patrícia Peck. **Direito Digital**. Editora Saraiva, 2021. E-book. ISBN 9786555598438. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555598438/. Acesso em: 25 out. 2023.

PRADO, Geraldo. **A cadeia de custódia da prova no processo penal**. São Paulo: Marcial Pons, 2021.

REALE, Miguel. **Lições preliminares de direito.** São Paulo: Saraiva, 2012.

REED, Chris. How should we regulate artificial intelligence?. **Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences**, v. 376, n. 2128, p. 20170360, 2018.

RINCON-SALCEDO, Javier Gustavo. REPENSAR EL DERECHO. **Int. Law: Rev. Colomb. Derecho Int.**, Bogotá, n. 26, p. 9-11, June 2015.

ROSINA, Mônica. Seminário Internacional Fake News e Eleições [recurso eletrônico]: anais. Brasília: Tribunal Superior Eleitoral, 2019. p.177. Disponível em: https://www.tse.jus.br/hotsites/catalogo-publicacoes/pdf/livro-digital-fake-news.pdf. Acesso em: 07 Jan 2024.

ROXIN, Claus. **Derecho procesal penal**. Buenos Aires: Editores Del Puerto, 2003.

SCHERER, Matthew U. Regulating artificial intelligence systems: Risks, challenges, competencies, and strategies. **Harv. JL & Tech**., v. 29, 2015.

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

Scientific Working Group on Digital Evidence (SWGDE), International Organization on Digital Evidence (IOCE). Digital Evidence: Standards and Principles, **Forensic Science Communications**, V 2, N 2, April 2000. Disponível em: https://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm. Acesso em: 12 de fev. 2023

SIMONS, Josh. Algorithms for the People: Democracy in the Age of AI**. Princeton University Press**, 2023.

SOUZA, Déborah da Paz. **Proteção de dados e o processo penal: desafios e parâmetros da cadeia de custódia da prova digital**. 2021. Trabalho de Conclusão de Curso (Graduação em Direito) - Curso de Direito, Faculdade de Direito da Universidade de Brasília, Brasília, 2021. Disponível em: https://bdm.unb.br/bitstream/10483/28900/1/2021_DeboraDaPazSouza_tcc.pdf. Acesso em 30 set. 2022.

TAMER, Maurício Antonio. **O princípio da inafastabilidade da jurisdição no Direito Processual Civil Brasileiro**. Rio de Janeiro: LMJ Mundo Jurídico, 2017.

TÁVORA, Nestor; ALENCAR, Rosmar Rodrigues. **Curso de Processo Penal e Execução Penal**. 14. ed. Salvador: JusPodivm, 2019.

THAMAY, Rennan; TAMER, Maurício. **Provas no Direito Digital**: conceito da prova digital, procedimentos e provas digitais em espécie. São Paulo: Thomson Reuters Brasil, 2022.

THEODORO JUNIOR, Humberto. **Curso de Direito Processual Civil**. Rio de janeiro: Forense, 2018.

TROULLINOU, Pinelopi. Rethinking privacy and freedom of expression in the digital era: an interview with Mark Andrejevic. **Westminster Papers in Communication and Culture**, v. 12, n. 3, p. 72-77, 2017.

TURNER, Jacob. **Robot rules: Regulating artificial intelligence**. Springer, 2018.

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.

WILKINSON, Sue; HAAGMAN, D. Good practice guide for computer-based electronic evidence. **Association of Chief Police Officers**, 2010.