7 Information Society and Law

FMU
CENTRO UNIVERSITÁRIO

Anais do 7º Congresso Internacional Information Society and Law: Inteligência Artificial e seus desafios éticos e jurídicos no século XXI

Realização

Programa de Mestrado em Direito da Sociedade da Informação do Centro Universitário das Faculdades Metropolitanas Unidas – FMU

Greice Patrícia Fuller; Marcus Vinicius Moreira Zittei; Nivaldo Sebastião Vicola; Tiago Cappi Janini

(Organizadores)

Tiago Cappi Janini

(Editor)

Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)

7º Congresso Internacional Information Society and Law (11. : 2024 : São Paulo, SP)
Anais do 7º Congresso Internacional Information Society and Law [livro eletrônico] : Inteligência Artificial e seus desafios éticos e jurídicos no Século XXI / Greice Patrícia Fuller ... [et al.] organizadores. -- 1. ed. -- São Paulo : Ed. dos Autores, 2025. -- (Anais ; 1)
PDF

Outros organizadores: Marcus Vinicius Moreira Zittei, Nivaldo Sebastião Vicola, Tiago Cappi Janini
Vários autores.
Bibliografia
ISBN 978-65-01-72209-2

1. Direito 2. Inteligência artificial - Direito 3. Sociedade da informação 4. Sociedade da informação - Aspectos jurídicos I. Fuller, Greice Patrícia. II. Zittei, Marcus Vinicius Moreira. III. Vicola, Nivaldo Sebastião. IV. Janini, Tiago Cappi. V. Série.

25-305668.0 CDU-34:007

Índices para catálogo sistemático:

1. Sociedade da informação : Direito 34:007

Maria Alice Ferreira - Bibliotecária - CRB-8/7964

COMISSÃO ORGANIZADORA

Profa. Dra. Greice Patrícia Fuller (FMU)
Prof. Dr. Marcus Vinicius Moreira Zittei (FMU)
Prof. Dr. Nivaldo Sebastião Vicola (FMU)
Prof. Dr. Tiago Cappi Janini (FMU)

COMITÊ CIENTÍFICO

Profa. Dra. Ana Maria Viola de Sousa (UNIVAP)
Prof. Dr. Angelo Anzalone (Universidade de Cordoba/Espanha)
Prof. Dr. Carlos Renato Cunha (Universidades Londrina)
Prof. Dr. Émerson Penha Malheiro (FMU)
Prof. Dr. Fábio Romeu Canton Filho (FMU)
Prof. Dr. Felipe Marquette de Sousa (Universidade de Pisa/Itália)
Profa. Dra. Greice Patrícia Fuller (FMU)
Prof. Dr. Irineu Francisco Barreto Junior (FMU)
Prof. Dr. Jorge Shiguemitsu Fujita (FMU)
Prof. Dr. Lafayette Pozzoli (PUC/SP)
Prof. Dr. Luiz Eduardo Alves de Siqueira (FMU)
Prof. Dr. Marcus Vinicius Moreira Zittei (FMU)
Profa. Dra. Maria de Fátima Ribeiro (UNIMAR)
Prof. Dr. Nivaldo Sebastião Vicola (FMU)
Profa. Dra. Regina Vera Villas Bôas (PUC/SP)
Prof. Dr. Ricardo Pinha Alonso (UENP/UNIMAR)
Profa. Dra. Samyra Haydêe Dal Farra Naspolini (FMU)
Prof. Dr. Tiago Cappi Janini (FMU)
Prof. Dr. Vladimir Brega Filho (UENP)

PROGRAMAÇÃO

Dia 1 | 06 de novembro de 2024

9h - Mesa de abertura

Ricardo Ponsirenas - Magnífico Reitor do Centro Universitário das Faculdades Metropolitanas Unidas – FMU.

Marcus Vinicius Moreira Zittei - Coordenador do mestrado em Direito da Sociedade da Informação das Faculdades Metropolitanas Unidas – FMU. Coordenador Científico do Evento.

Cauê Nogueira de Lima - Coordenador do curso de graduação em Direito das Faculdades Metropolitanas Unidas - FMU.

Greice Patrícia Fuller - Professora do mestrado em Direito da Sociedade da Informação e coordenadora geral científica do evento - FMU.

Nivaldo Sebastião Vicola - Professor do mestrado em Direito da Sociedade da Informação e coordenador executivo do evento – FMU.

Tiago Cappi Janini - Professor do mestrado em Direito da Sociedade da Informação e coordenador executivo do evento - FMU.

9h30 - Painel de abertura

Profª. Drª. Sylvia Steiner - Mestre em Direito Internacional pela Faculdade de Direito da USP, foi desembargadora do Tribunal Regional Federal da 3ª Região e procuradora regional da República. Única brasileira a ter integrado o Tribunal Penal Internacional, exercendo mandato de 2003 a 2009.

14h às 17h - Grupos de trabalho

GT 02. Ética da Inteligência Artificial: Responsabilidade e Proteção de Dados em Sistemas Automatizados.

Coordenadores: Prof. Dr. Fabio Romeu Canton Filho; Prof. Dr. Irineu Francisco Barreto Junior e Prof. Dr. Tiago Cappi Janini

19h às 21h30 - Painel 1

Profª. Drª. Lucineia Rosa Dos Santos (Brasil) - Doutora em Direitos Humanos pela PUC/SP, mestre em Direito do Trabalho pela mesma instituição e professora de Direitos Humanos e ECA na PUC/SP.

Prof. Dr. José Luis Batiz (México) - Doutor em Direito da Sociedade Global pela Universidade de Navarra (Espanha). Mestre em Direito Internacional, Comércio Exterior e Relações Internacionais pelo Instituto de Direito e Economia em Madri. Professor na Faculdade de Ciências Administrativas e Sociais da Universidade Autónoma de Baja California.

Dia 2 | 07 de novembro de 2024

9h às 11h30 - Painel 2

Prof. Dr. Eduardo Valpuesta (Espanha) - Professor catedrático de Direito Mercantil na Universidade de Navarra e coordenador do mestrado e doutorado em Direito Digital da Universidade de Navarra (Espanha).

Prof. Dr. Jorge Andrés Castilho (Colombia) - Doutor em Contabilidade e Finanças Corporativas pela prestigiada Universidade de Valência (Espanha). Professor na Universidade Militar de Nova Granada.

14h às 17h - Grupos de trabalho

GT 01. IA no Poder Judiciário e o papel dos algoritmos.

Coordenador: Prof. Dr. Luiz Eduardo Siqueira (FMU).

19h às 21h30 - Painel 3

Prof. Dr. Rolando Rosas (México) - Titular da Unidade de Investigações Cibernéticas e Operações Tecnológicas do Ministério Público Federal do México.

Prof. Dr. Bruno Cogan (Brasil) - Doutor e mestre em Processo Penal pela Pontifícia Universidade Católica de São Paulo (PUC/SP). Delegado de Polícia da Polícia Civil do Estado de São Paulo. Professor do Departamento de Direito Penal e Processual Penal da PUC/SP.

Dia 3 | 08 de novembro de 2024

9h às 11h30 - Painel 4

Profª. Drª. Tainá Aguiar Junquilho (Brasil) - Lançamento do documentário Jurismáquina.

Doutora pela Universidade de Brasília (em IA e Direito), mestre em Direito pela Universidade Federal do Espírito Santo (UFES). Professora de Tecnologia, Inovação e Direito no Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP). Assistente parlamentar no Senado Federal.

14h às 17h - Grupos de trabalho

GT 03. Discriminação e violações de Direitos Humanos pelo Algoritmo.

Coordenadores: Prof. Dr. Nivaldo Sebastião Vícola; Profª Drª Samyra Haydêe Dal Farra Naspolini e Prof. Dr. Wanderley Andrade da Costa Lima.

GT 04. Inteligência Artificial e o impacto nas relações de trabalho e de direito privado.

Coordenador: Prof. Dr. Jorge Shiguemitsu Fujita.

GT 05. IA e a tutela penal em face da dignidade da pessoa humana.

Coordenadores: Profª. Drª. Greice Patricia Fuller e Prof. Ms. Fabio Gallinaro.

19h às 21h30 - Painel 5

Prof. Dr. Wilson Engelmann (Brasil) - Pós-doutor pela Faculdade de Direito da Universidade de Santiago de Compostela, Espanha. Doutor e mestre em Direito pela Unisinos. Professor e pesquisador do Mestrado Profissional em Direito da Empresa e dos Negócios na Universidade do Vale do Rio dos Sinos (Unisinos). Professor e pesquisador do Programa de Pós-Graduação em Direito (mestrado e doutorado) na Unisinos.

Prof. Dr. Diego Platz Pereira (Brasil/Alemanha) - Doutorando em Direito pela Universidade de Münster, Alemanha. Assistente de pesquisa no Departamento de Teoria do Estado, Ciências Políticas e Direito Constitucional Comparado da

Universidade de Göttingen, Alemanha. Mestre em Direito pela Universidade de Münster.

Clausura final

Prof. Dr. Marcus Zittei - Coordenador do Programa de Mestrado em Direito da Sociedade da Informação.

SUMÁRIO

GT 01. IA NO PODER JUDICIÁRIO E O PAPEL DOS ALGORITMOS.

Coordenador: Prof. Dr. Luiz Eduardo Siqueira (FMU).

Artigos

A influência da inteligência artificial nos trâmites processuais do Poder Judiciário brasileiro.....13

Carlos Susumu Thomioka

Resumos Expandidos

A racionalização formal e burocrática através dos mecanismos de inteligência artificial do Poder Judiciário brasileiro..... 30

Gustavo Rubio Claret Pereira

A inteligência artificial e os algoritmos no poder judiciário.....37

Luiz Eduardo Alves de Siqueira

GT 02. ÉTICA DA INTELIGÊNCIA ARTIFICIAL: RESPONSABILIDADE E PROTEÇÃO DE DADOS EM SISTEMAS AUTOMATIZADOS.

Coordenadores: Prof. Dr. Fabio Romeu Canton Filho; Prof. Dr. Irineu Francisco Barreto Junior e Prof. Dr. Tiago Cappi Janini

Artigos

Uso da inteligência artificial na fiscalização tributária e seus efeitos sobre os direitos fundamentais....45

Stefanie Cristine Kulkas da Silva

Digitalização e teoria da prova: uma análise contemporânea.....62

Edielma Rocha Dutra e Tiago Cappi Janini

Sociedade da informação e os novos paradigmas do direito: crimes cibernéticos, privacidade e acesso à informação.....86

Edielma Rocha Dutra e Kelly Cristina Maciel da Silva Costa

Resumos Expandidos

A regularização jurídica brasileira voltada à utilização de robôs.....114
Ronny Max Machado e João Francisco Mantovanelli

Equipamentos inteligentes: impactos da IOT na vida cotidiana, privacidade e segurança....120
Ronny Max Machado e Francisco Céu Pereira

Inteligência artificial no dia a dia com ética e responsabilidade na era digital.....126
Sara Pereira Guimarães

Inteligência artificial e governança - uma necessidade global.....133
Flavio Cesar Vasconcellos Ferreira

Teoria crítica do direito: desvelando as estruturas de poder e emancipação na era digital....142
Edielma Rocha Dutra e Paula Aline Aguiar Gozi

Treinamento de inteligência artificial com dados de navegação em redes sociais:
abordagens, implicações éticas e impacto na privacidade dos usuários..... 152
Claudia Silva de Oliveira Camargo

GT 03. DISCRIMINAÇÃO E VIOLAÇÕES DE DIREITOS HUMANOS PELO ALGORITMO.

Coordenadores: Prof. Dr. Nivaldo Sebastião Vícola; Profª Drª Samyra Haydêe Dal Farra Naspolini e Prof. Dr. Wanderley Andrade da Costa Lima.

Artigos

Discriminação e violações de direitos humanos pelo algoritmo.....160
Eduardo Tognetti

Automação no judiciário: potenciais riscos e o papel da inteligência artificial.....172
Sofia Martins Rangel Garcia

O conto da IA: a violência de gênero algorítmica e os direitos humanos.....181
Ellen Maria Rocha da Silva

Resumos Expandidos

Fake news e sociedade da informação: as condutas do candidato à prefeitura de São Paulo Pablo Henrique Marçal na eleição municipal de São Paulo de 2024..... 201
Ronny Max Machado e João Francisco Mantovanelli

Discriminação e violações de direitos humanos pelo algoritmo nos Estados Unidos..... 207
Bruna Matos de Souza e Claudio Luiz de Carvalho

GT 04. INTELIGÊNCIA ARTIFICIAL E O IMPACTO NAS RELAÇÕES DE TRABALHO E DE DIREITO PRIVADO.

Coordenador: Prof. Dr. Jorge Shiguemitsu Fujita.

Artigos

A inteligência artificial e os direitos das pessoas e do meio ambiente: tecnologia, inovação, sustentabilidade e efetividade..... 217
Regina Vera Villas Bôas e Tiago Cappi Janini

Inteligência artificial e o impacto nas relações de trabalho..... 227
Selma Strublic

Trajetória epistemológica da relação entre teoria geral de sistemas, gestão de riscos e governo eletrônico.....239
Marcus Vinicius Moreira Zittei

A inteligência artificial, o desemprego e a falta de regulamentação no Brasil..... 262
Luís Filipe Fernandes Ferreira

GT 05. IA E A TUTELA PENAL EM FACE DA DIGNIDADE DA PESSOA HUMANA.

Coordenadores: Profª. Drª. Greice Patricia Fuller e Prof. Ms. Fabio Gallinaro.

Artigos

A inteligência artificial como instrumento no combate aos
crimes digitais na área médica..... 282
Rodrigo de Carvalho Gonçalves Júnior

Prova pericial, cadeia de custódia e evidências digitais: desafios na era da informação.....291
André Luiz Viana Borges; Cassia Luize Ferreira da Silva e Irineu Francisco Barreto Junior

Uso da inteligência artificial para criação de conteúdo sexual infantil:
a expansão da pedofilia virtual.....312
Mariana Pereira Marques

APRESENTAÇÃO

É com imensa alegria que apresentamos os Anais do *7º Congresso Internacional Information Society and Law*, organizado pelo Programa de Mestrado em Direito da Sociedade da Informação das Faculdades Metropolitanas Unidas (FMU), realizado nos dias 6 a 8 de novembro de 2024.

O Congresso é destinado a docentes, pesquisadores e outros profissionais, assim como alunos de graduação e pós-graduação, com o objetivo de fomentar a discussão acadêmica de temas relacionados com o Direito da Sociedade da Informação, que, nesta edição, teve como eixo central "Inteligência Artificial e seus desafios éticos e jurídicos no século XXI".

Em um mundo marcado por transformações tecnológicas que impactam profundamente o Estado e a sociedade em suas múltiplas relações, o protagonismo recente da Inteligência Artificial requer a atenção dos pesquisadores para analisar o seu envolvimento com o sistema jurídico.

Esperamos, com o *7º Congresso Internacional Information Society and Law*, contribuir com a reflexão sobre os desafios apresentados pela Inteligência Artificial dentro do contexto da Sociedade da Informação, em uma proposta multidisciplinar, englobando não só o direito, mas outras áreas do saber.

Ótima leitura!

Comissão Organizadora

7 Information Society and Law
FMU CENTRO UNIVERSITÁRIO

A INFLUÊNCIA DA INTELIGÊNCIA ARTIFICIAL NOS TRÂMITES PROCESSUAIS DO PODER JUDICIÁRIO BRASILEIRO

THE INFLUENCE OF ARTIFICIAL INTELLIGENCE ON THE PROCEDURAL PROCEEDINGS OF THE BRAZILIAN JUDICIARY

Carlos Susumu Thomioka[1]

Resumo: Este artigo examina o impacto da inteligência artificial (IA) nos processos judiciais no Brasil, considerando seu potencial para aumentar a eficiência, reduzir custos e agilizar a gestão de casos. São analisadas iniciativas-chave como o Projeto Victor do STF, juntamente com exemplos internacionais como o ROSS nos Estados Unidos e o uso da IA em processos judiciais na Australia e no Reino Unido. Adicionalmente, explora-se a aplicação da IA em recursos repetitivos, IAC e IRDR nos tribunais superiores brasileiros. A análise enfatiza os princípios de economicidade, eficiência, questões éticas e de direitos humanos, destacando a importância de prevenir o viés algorítmico e garantir a supervisão e accountability. São abordados dilemas éticos, desafios futuros e os riscos da justiça automatizada para os direitos humanos. A conclusão oferece recomendações para a implementação e regulamentação da IA no Judiciário, ressaltando a necessidade de equilibrar a inovação tecnológica com a salvaguarda das garantias constitucionais.
Palavras-chave: Inteligência Artificial, Judiciário, Processos Judiciais, Viés Algorítmico, Automação da Justiça

Abstract: This paper examines the impact of artificial intelligence (AI) on judicial processes in Brazil, considering its potential to increase efficiency, reduce costs, and streamline case management. Key initiatives such as the Supreme Court's Victor Project are analyzed, alongside international examples such as ROSS in the United States and AI usage in judicial processes in Australia and the United Kingdom. Additionally, the application of AI in repetitive appeals, IAC, and IRDR within Brazil's higher courts is explored. The analysis emphasizes economic principles, efficiency, ethical considerations, and human rights, drawing attention to the importance of preventing algorithmic bias and ensuring supervision and accountability. Ethical dilemmas, future challenges, and the risks posed by automated justice to human rights are also addressed. The conclusion offers recommendations for the implementation and regulation of AI in the judiciary, highlighting the need for a careful balance between technological innovation and the safeguarding of constitutional guarantees.
Keywords: Artificial Intelligence, Judiciary, Judicial Processes, Algorithmic Bias, Justice Automation.

[1] Formado como bacharel em Sistemas de Informação na Universidade Presbiteriana Mackenzie em 2004. Formado como Técnico em Eletrotécnica pela Escola Técnica Federal de São Paulo em 1994.

1. INTRODUÇÃO

O presente artigo tem como objetivo discutir o impacto da Inteligência Artificial (IA) no contexto jurídico, especialmente na forma como pode influenciar as decisões processuais. Inicialmente, será abordado o conceito de IA explorando suas principais subdivisões: IA forte e IA fraca, além de apresentar o machine learning (aprendizado de máquina), uma das tecnologias mais proeminentes nesse campo. A partir dessas definições, será possível compreender como os sistemas de IA têm evoluído para automatizar tarefas que antes dependiam exclusivamente da inteligência humana.

Outro ponto central deste estudo é o viés algorítmico, fenômeno que ocorre quando os dados utilizados para treinar os algoritmos de IA carregam preconceitos ou desigualdades presentes na sociedade, influenciando diretamente o comportamento dessas máquinas. A combinação desses fatores – IA, machine learning e viés algorítmico – será analisada quanto à sua aplicação nos processos judiciais no Brasil, buscando entender como podem impactar as decisões relacionadas aos pleitos apresentados pelas partes.

A proposta é, portanto, refletir sobre as possíveis vantagens, desvantagens e desafios que a IA traz ao sistema judicial, tanto em termos de eficiência quanto de justiça, ao automatizar e influenciar decisões em processos complexos e, muitas vezes, determinantes para a vida das pessoas.

2. A INTELIGÊNCIA ARTIFICIAL

A inteligência artificial é um ramo da ciência da computação que busca criar sistemas capazes de realizar tarefas que normalmente precisariam de inteligência humana. Isso inclui reconhecer voz, entender imagens, tomar decisões e, mais recentemente, aprender com a experiência, algo que chamamos de aprendizado de máquina. A IA pode ser dividida em duas categorias principais: IA forte e IA fraca.

A IA forte é aquela que, em teoria, teria consciência e entenderia o mundo como um ser humano. No entanto, essa ideia ainda está no campo da especulação e da ficção científica, sendo algo que não alcançamos. Já a IA fraca se refere a sistemas que são feitos para executar tarefas específicas de maneira eficiente, mas sem qualquer compreensão real do que estão fazendo. A maioria das Inteligências Artificiais que usamos hoje, como assistentes virtuais e sistemas de recomendação, pertence a essa categoria (Russell & Norvig, 2021).

Dentro da IA fraca, um dos componentes mais importantes é o aprendizado de máquina (ou machine learning). De acordo com Mitchell (1997), o aprendizado de máquina envolve o uso de algoritmos que melhoram com a experiência, ou seja, que ficam mais "inteligentes" à medida que processam mais dados. Esses algoritmos permitem que sistemas de IA identifiquem padrões e tomem decisões sem que os programadores precisem ensinar cada passo. Isso já está sendo aplicado em muitas áreas, como na saúde, nos bancos e no Judiciário.

No entanto, o uso da IA, especialmente do aprendizado de máquina, também traz alguns desafios importantes, como o **viés algorítmico**. Falando nisso, temos que saber o que é um **algoritmo** que é definido por uma sequência de instruções ou passos bem definidos que são seguidos para resolver um problema ou realizar uma tarefa. Em termos simples, é como se fosse uma receita de bolo: um conjunto de instruções que você segue para obter um resultado específico. No mundo da computação, os algoritmos são usados para processar dados, realizar cálculos, tomar decisões e automatizar tarefas.

O viés algorítmico acontece quando os dados usados para treinar os sistemas de IA refletem desigualdades ou preconceitos da sociedade. Buolamwini e Gebru (2018) analisaram sistemas de reconhecimento facial e descobriram que esses algoritmos funcionam melhor para homens brancos e nem tanto para mulheres negras. Isso mostra como a IA pode, sem querer, reforçar discriminações se não for bem controlada.

Outro uso da inteligência artificial seria os **chatbots**. Chatbots são programas de computador que simulam uma conversa com um ser humano por meio de mensagens de texto ou voz. Eles são usados para responder a perguntas, ajudar em tarefas e fornecer informações de forma automática. Imagine como se você estivesse conversando com um robô que entende o que você diz e responde de forma rápida e clara (Russell & Norvig, 2021).

Por exemplo, quando você entra em um site de uma loja e vê uma janela de bate-papo aparecendo, oferecendo ajuda para tirar dúvidas, isso provavelmente é um chatbot. Ele pode te ajudar a encontrar produtos, explicar políticas da loja, ou até mesmo processar pedidos de compras. Outro exemplo comum é o assistente virtual em serviços bancários, como o usado no app (aplicativo de celular) do seu banco para te ajudar a conferir saldo ou fazer transferências.

Existem também chatbots em aplicativos de mensagens, como o WhatsApp ou o Messenger do Facebook, onde empresas ou serviços automatizados respondem perguntas sobre

horários de atendimento, localização de lojas, ou até resolvem problemas de suporte técnico. Outros exemplos de chatbots que são realidade entre nós, que podem ser mencionados seriam:

- **Siri (Apple)** ou **Google Assistant** que são chatbots que funcionam por voz. Eles respondem a comandos e perguntas dos usuários, como "Qual é a previsão do tempo?" ou "Toque uma música";
- **Chatbots de atendimento ao cliente**, como os que encontramos em sites de lojas, podem ajudar a tirar dúvidas sobre produtos ou realizar tarefas básicas como rastrear pedidos;
- **Chatbots no WhatsApp**, como o usado por algumas empresas de telecomunicações, ajudam os clientes a verificarem pacotes de dados ou pagar contas diretamente pelo aplicativo.

3. A INTELIGÊNCIA ARTIFICIAL E SEUS USOS NO JUDICIÁRIO

3.1. Automatização de processos

A IA tem o potencial de transformar significativamente a triagem processual no Brasil e no mundo. Países como os EUA já utilizam algoritmos para auxiliar na análise de litígios, como nos casos de pequenas causas. Entre os principais benefícios conquistados, destacam-se:

- **Aumento da eficiência**: algoritmos de IA podem processar grandes volumes de dados rapidamente, acelerando a tramitação de processos;
- **Automatização de tarefas repetitivas**: atividades como classificação de documentos, análise de petições e verificação de requisitos processuais podem ser realizadas de forma automática, liberando magistrados e servidores para tarefas mais complexas;
- **Desafogamento do Judiciário**: conforme o entendimento de Alves (2022), o investimento de softwares e inteligência artificial tem demostrado ser uma excelente ferramenta na gestão processual, como tentativa de combater a morosidade processual e aumentar a produtividade.
- **Agilidade e eficiência**: segundo o CNJ (2024), "entre os principais motivadores para criar um projeto de IA estão a busca por eficiência e agilidade, o aumento da precisão e consistência de tarefas repetitivas, e o empenho por inovação nos processos internos, melhoria na tomada de decisões e redução de erros".
- **Precisão e redução de erros**: a utilização de IA na revisão de documentos e na identificação de precedentes pode reduzir a margem de erro nas decisões, conforme dito pelo CNJ (2024).

A automação desempenha um papel essencial na eficiência do Judiciário. O sistema PJe (Processo Judicial Eletrônico) tem utilizado algoritmos para a triagem de processos, categorizando-os e alocando-os para as varas competentes.

Segundo o CNJ, é promulgada no final de 2013, a Resolução 185 do CNJ que institui o **Sistema Processo Judicial Eletrônico – PJe** como sistema de processamento de informações e prática de atos processuais e estabelece os parâmetros para sua implementação e funcionamento. O PJe é caracterizado pela proposição da prática de atos jurídicos e acompanhamento do trâmite processual de forma padronizada, mas considerando características inerentes a cada ramo da Justiça. Tem como função a conversão de esforços para a adoção de solução padronizada e gratuita aos Tribunais, que atenta à racionalização aos ganhos de produtividade nas atividades do judiciário, e aos gastos com elaboração ou aquisição de softwares, permitindo o emprego de recursos financeiros e de pessoal em atividades dirigidas à finalidade do Judiciário.

3.2. Análise preditiva

Análise preditiva é um tipo de análise de dados que usa informações do passado para prever o que pode acontecer no futuro. Encare a análise preditiva como se fosse uma "bola de cristal" que, em vez de magia, usa estatísticas e algoritmos para fazer previsões.

Por exemplo, imagine uma loja que tem registros de vendas de anos anteriores. Usando análise preditiva, ela pode identificar padrões e prever quantas pessoas vão comprar um produto específico no próximo mês, com base no comportamento de compras passadas, épocas do ano e até fatores como o clima.

Na realidade, há exemplos do uso deste recurso, como por exemplo, grandes empresas de streaming, como a Netflix, usam análise preditiva para sugerir filmes e séries que você pode gostar. Eles têm as informações sobre o que você assistiu no passado e para as preferências de milhões de outros usuários com gostos parecidos para prever o que você pode querer ver a seguir, traçando uma espécie de perfil com gostos e preferências. Isso melhora a experiência do usuário e mantém as pessoas mais engajadas. Em resumo, a análise preditiva ajuda empresas e pessoas a tomar decisões mais inteligentes ao usar dados do passado para antecipar o futuro, de acordo com Siegel (2013).

Conforme as afirmações de Schuchowsky (2024), a Inteligência Artificial pode realizar análises preditivas com base em dados históricos. Com o emprego de algoritmos avançados, a IA pode prever resultados judiciais, identificar tendências legais e até mesmo

antecipar potenciais conflitos. Essa capacidade permite que os advogados tomem decisões mais informadas e estratégicas, melhorando a eficácia de sua representação.

Exemplo disso é o **Projeto Victor**, do Supremo Tribunal Federal (STF), que é uma iniciativa real de inteligência artificial que visa ajudar na triagem de recursos extraordinários. Essa ferramenta utiliza análise preditiva para otimizar o processo de decisão do tribunal, analisando a admissibilidade de recursos e aumentando a eficiência do julgamento de casos repetitivos. "O Victor é uma inteligência artificial voltada para apoiar a atividade de análise de admissibilidade recursal, mediante sinalização de que um dado tema de repercussão geral, ou mais de um, se aplica ao caso dos autos. Trata-se, portanto, de um indicativo que sempre é validado ou confirmado durante a efetiva apreciação do caso concreto pelos ministros" (STF, 2021).

Essa ferramenta é crucial para reduzir a sobrecarga do STF, especialmente em temas de alta complexidade e com grande volume de ações.

3.3. IA internacional: ROSS e processos judiciais na Estônia e Reino Unido

Conforme explica Alves (2022), a startup canadense ROSS Intelligence em colaboração com a Universidade de Toronto em 2016 criou através da plataforma de machine learning, o primeiro robô advogado chamado de **ROSS**, por meio da plataforma Watson, da IBM. Esse sistema é capaz de ouvir a linguagem humana, rastrear mais de 10 mil páginas por segundo e formular respostas muito mais rápido do que qualquer profissional do Direito. Os algoritmos desse robô permitem que ele identificar a ideologia da autoridade judicial, as partes envolvidas no julgamento e os tribunais de onde vêm os casos. Além disso, também é capaz de rastrear novas legislações, caso haja mudanças legislativas no mesmo instante que elas ocorrerem.

Isso foi um grande atrativo para que grandes escritórios de advocacia ao redor do mundo como Baker & Hostetler e o Pierce Bainbridge fossem atrás do robô advogado para impulsionar a produtividade em seus escritórios. O Ross é capaz de rastrear em tempo real os resultados de julgamentos para alertar os advogados sobre qualquer novidade que possa representar um risco ou uma ameaça aos clientes. O robô também tem o poder de interpretar a jurisprudência a partir de casos armazenados em seu banco de dados. Além disso, o robô é capaz de escanear e prever quais documentos serão relevantes para um caso concreto.

Segundo Negreiro (2023), no Reino Unido, existem plataformas online estão usando IA para resolver disputas legais de maneira mais acessível e eficiente. Por exemplo, o **Resolve Disputes Online - RDO** consiste em que as partes resolvam disputas de pequenas quantias sem a necessidade de comparecer a um tribunal físico. Esta plataforma usa a IA para facilitar a comunicação entre as partes e guiar o processo de resolução. Isso economiza tempo e dinheiro para todas as partes envolvidas, tornando a justiça mais acessível.

Negreiro comenta que em certas áreas geográficas remotas, onde a presença de advogados é limitada, a Inteligência Artificial é usada para fornecer assistência jurídica à distância, como é o caso da Austrália com o **Rural, regional, and Remote Law - RRRL** que utiliza plataformas de videoconferência e IA para conectar advogados com clientes em áreas rurais. Isso permite que as pessoas obtenham aconselhamento jurídico sem a necessidade de viajar longas distâncias até um escritório de advocacia

4. PRINCÍPIOS PROCESSUAIS DO CPC DE 2015, DA CONSTITUIÇÃO FEDERAL E A INTELIGÊNCIA ARTIFICIAL

4.1. Princípio da Igualdade (art. 7º, CPC; art. 5º, CF)

A IA possui o potencial de democratizar o acesso à justiça ao oferecer recursos legais acessíveis e compreensíveis para um público mais amplo. Chatbots jurídicos e assistentes virtuais podem orientar os indivíduos em questões legais simples, oferecendo informações básicas e direcionando para recursos adicionais, conforme Schuchowsky (2024).

4.2. Princípio da Dignidade Humana (art. 8º, CPC; art. 1º, III, CF)

A tecnologia deve ser usada de forma que não desrespeite a dignidade humana, tratando cada caso com a importância que ele merece.

O art. 8º do CPC de 2015, que estabelece que o juiz deve respeitar a dignidade da pessoa humana, observando os princípios tocantes à proporcionalidade, razoabilidade, legalidade, a publicidade e a eficiência

4.3. Devido Processo Legal (art. 5º, LIV, CF)

O devido processo legal é fundamental para garantir que todos os indivíduos tenham a oportunidade de se defender e de apresentar suas provas. A Inteligência Artificial pode

auxiliar no monitoramento de prazos e na organização de documentos, mas deve sempre respeitar o direito de defesa.

Mas, sem a presença da imparcialidade nos julgados (decisões enviesadas pelos algoritmos de IA), a adoção da interpretação humana das normas, a análise da particularidade dos casos, a individualização da pena e a carência de transparência nos julgados, acaba-se violando princípios básicos da jurisdição brasileira, inclusive consubstanciados nos Direitos Humanos expressamente previstos na Declaração Universal dos Direitos Humanos e, consequentemente, opera-se também a violação ao devido processo legal (Travizani, et al., 2021).

4.4. Princípio da Cooperação (art. 6º, CPC)

Quando aplicado ao uso da Inteligência Artificial (IA) no Judiciário brasileiro, o princípio da cooperação se traduz na forma como as tecnologias de IA são integradas aos processos judiciais, promovendo a cooperação entre as partes para garantir um processo mais célere e eficaz. Esse princípio também se reflete na colaboração entre os tribunais, ao compartilhar soluções tecnológicas, dados e melhores práticas. O compartilhamento de ferramentas é uma das premissas do Programa Justiça 4.0, que aposta no modelo colaborativo para a gestão mais eficiente de recursos e integração de soluções, como afirma o CNJ (2022).

4.5. Economicidade Processual e Duração Razoável do Processo (art. 4º, CPC; art. 5º, LXXVIII, CF)

A economicidade processual é um conceito implícito no ordenamento jurídico brasileiro, derivado do dever de eficiência previsto no caput do art. 37 da Constituição Federal e na busca pela celeridade processual. A IA pode contribuir significativamente para o cumprimento desse princípio no Judiciário. A automação da triagem processual permite que o tempo e os recursos sejam utilizados de maneira mais racional, com a ferramenta lidando com grandes volumes de dados e processos em pouco tempo. Isso contribui para a melhoria do desempenho do sistema judicial e atende ao princípio da celeridade processual, previsto no art. 4º do CPC, que busca evitar a demora excessiva nos julgamentos.

Entre fevereiro e agosto de 2020, o Judiciário tinha 64 projetos de IA em funcionamento ou em processo de implantação, em 47 tribunais do país, além da Plataforma Sinapses do CNJ. “Metade dos tribunais têm um projeto de inteligência artificial implantado ou

em implantação. O desenvolvimento dessas tecnologias é um dos instrumentos mais importantes de gestão no Judiciário, uma vez que implica em racionalizar recursos, mão de obra e atividades, diante de uma demanda cada vez mais crescente", na fala do ministro do Superior Tribunal de Justiça (STJ) Luís Felipe Salomão, coordenador do Centro de Inovação, Administração e Pesquisa do Judiciário, da Fundação Getúlio Vargas - FGV, conforme CNJ (2021).

4.6. Princípio da celeridade processual (art. 4º, CPC)

A celeridade processual é um dos pilares da justiça, e a Inteligência Artificial tem um papel crucial nesse aspecto. A utilização de sistemas que otimizam a distribuição de processos e a análise de dados pode reduzir significativamente o backlog dos tribunais (acúmulo de processos que ainda não foram julgados ou finalizados).

Um exemplo disso é a implementação da ferramenta **Radar** no Tribunal de Justiça de Minas Gerais que identificou e separou recursos com idênticos pedidos, e permite a realização de julgamentos céleres. Com a plataforma Radar, os magistrados poderão fazer buscas inteligentes por filtros como palavra-chave, por data de distribuição, por órgão julgador, por magistrado, por parte, por advogado e por outras demandas que os julgadores necessitarem (TJ-MG, 2018).

4.7. Princípio da inafastabilidade de jurisdição (art. 5º, XXXV, CF)

O princípio da inafastabilidade assegura que nenhum lesado ficará sem acesso à justiça. A Inteligência Artificial quando utilizada para facilitar processos, pode garantir que as causas sejam ouvidas. Contudo, deve-se enfatizar que o uso da tecnologia não deve excluir métodos tradicionais que asseguram a acessibilidade da justiça, especialmente para aqueles sem familiaridade com ferramentas eletrônicas. A inafastabilidade pode ocorrer nessas três vertentes:

- **Automação de Decisões Judiciais**: A IA pode ser usada para automatizar tarefas processuais, como triagem de casos, análise de documentos e até mesmo sugestões de decisões. No entanto, o uso dessas tecnologias não pode substituir o papel do juiz humano, especialmente em casos que demandem discricionariedade e interpretação subjetiva. O CNJ, por meio da Resolução n. 332/2020, considerando os avanços da tecnologia, estabeleceu a implementação de mecanismos de Inteligência Artificial em âmbito judicial, considerando a promoção de bem-estar e a prestação equitativa com

uso da mencionada ferramenta, o que colabora diretamente com o acesso mais democrático à justiça, inclusive as Pessoas Com Deficiência - PCDs (CNJ, 2022).

- **Transparência e Controle sobre Decisões Automatizadas**: Um dos desafios na aplicação da IA no Judiciário é garantir que as partes entendam e possam contestar decisões feitas por algoritmos. Para que o princípio da inafastabilidade seja respeitado, é crucial que os sistemas de IA sejam transparentes e passíveis de revisão por humanos, possibilitando o controle judicial sobre as decisões automatizadas.
- **Acesso Universal**: Embora a IA possa melhorar a eficiência dos tribunais, é importante que sua adoção não crie barreiras para o acesso à justiça, especialmente para populações vulneráveis que podem não ter familiaridade com a tecnologia. As ferramentas de IA devem ser desenvolvidas de forma inclusiva, garantindo que todos tenham a possibilidade de acessar o Judiciário de forma igualitária.

4.8. Recursos repetitivos, IAC E IRDR

A IA tem sido empregada no STJ, STF e nos demais tribunais para automatizar a triagem de recursos repetitivos, casos de Repercussão Geral, Incidentes de Assunção de Competência (IAC) e Incidentes de Resolução de Demandas Repetitivas (IRDR), otimizando a gestão de casos de grande volume.

O **Projeto Victor** do Supremo Tribunal Federal é uma inteligência artificial voltada para apoiar nas análises de admissibilidade recursal, mediante sinalização de que um dado tema de repercussão geral, ou mais de um, se aplica ao caso dos autos. (STF, 2021).

Segundo Olinda e Carvalho (2022), o **Accorde** do Superior Tribunal de Justiça (STJ) consegue identificar recursos que tenham o mesmo assunto, e que possam ser julgados como repetitivos, pacificando o tema no âmbito nacional e contribuindo para a uniformização da Jurisprudência. A utilização de IA na triagem de recursos repetitivos resultou em uma redução significativa no tempo de processamento desses casos, permitindo que a Corte se concentre em questões mais complexas.

No caso da IRDR, o Tribunal de Justiça de Goiás implementou uma aplicação de inteligência artificial para relacionar os novos processos com os IRDR já proferidos se tornaria uma ferramenta importante para os juízes, poderem agilizar o julgamento, vinculando processos relacionados já julgados e evitando julgamentos divergentes para processos relacionados. Para a integração, uma **API** (Interface de Programação de Aplicações), que é um conjunto de regras e protocolos que permite que diferentes sistemas ou aplicativos se comuniquem entre si, foi instalada e atualmente está funcionando no Tribunal de Justiça. Este trabalho propõe um método

de IA para representar computacionalmente documentos legais e um modelo para classificação de texto. Os resultados da simulação com valores de 93% de acurácia, 97% de precisão e 93%de recall indicam que o método de IA proposto foi bem-sucedido e traz confiança em sua aplicação em ambiente de produção na Justiça de Goiás (Castro Junior, 2022).

5. EXEMPLOS DE APLICAÇÃO DA IA NO STJ E TRIBUNAIS ESTADUAIS

Os tribunais superiores e estaduais têm avançado na implementação de ferramentas de IA. O STJ, por exemplo, utiliza um sistema de IA que ajuda na análise de jurisprudência e na identificação de precedentes relevantes para os casos em andamento (Olinda & Carvalho, 2022).

Outros tribunais, como o do Rio de Janeiro (TJ-RJ) e de Minas Gerais (TJ-MG), também implementaram soluções de IA para melhorar a eficiência na gestão de processos.

O Tribunal de Justiça de Minas Gerais (TJ-MG) implementou o Sistema de Orientação e Facilitação de Informações e Acessibilidade (SOFIA) tem a finalidade de esclarecer para os usuários do sistema de justiça o conteúdo das decisões judiciais, movimentações processuais e do vocabulário jurídico em geral, apoiando o cidadão na compreensão de forma simples e acessível, esclarecendo o teor de movimentações processuais e expressões. Com o uso de um celular, a partir da leitura de um QR Code que está no corpo dos documentos referentes a atos e peças processuais, como mandados, decisões e sentenças, onde o cidadão é conduzido para uma plataforma em tecnologia mobile que apresenta o resumo do documento em uma linguagem simples, sugestões de perguntas para outras dúvidas ou termos jurídicos, conforme o contexto do documento. A ferramenta é orientada por IA generativa e possui recursos que aumentam a acessibilidade do usuário, permitindo a inserção de informações por comando de voz e áudio para leitura das informações, através de Inteligência Artificial. O sistema promove a democratização do acesso à informação jurídica e aumenta a transparência no processo judicial (TJ-MG, 2023).

No final de agosto de 2024, o Tribunal de Justiça do Estado do Rio de Janeiro (TJ-RJ) lançou o **ASSIS**, uma ferramenta de suporte à jurisdição capaz de construir minutas de relatórios, decisões e sentenças em processos judiciais eletrônicos, através do uso da Inteligência Artificial generativa com seu uso ético e responsável, segundo o CNJ (2024).

6. RESISTÊNCIAS E CONFLITOS

A resistência por parte de profissionais do Direito e defensores dos Direitos Humanos representa um desafio significativo. Muitos juristas expressam preocupações sobre a perda de subjetividade nas decisões judiciais, temendo que a automação possa substituir a análise humana essencial em casos complexos. A questão ética se torna ainda mais pertinente com a possibilidade de discriminação algorítmica.

Não se pode deixar de mencionar que a defesa dos direitos fundamentais e sociais garantidos pela Constituição Federal de 1988, amplamente estabelecidos e divulgados no Estado Democrático de Direito, também contribui para o aumento da sobrecarga sobre o Poder Judiciário. Quando os indivíduos sentem que seus direitos foram lesados ou violados, buscam na justiça a busca por justiça, aumentando ainda mais o volume de casos a serem tratados pelo sistema judiciário brasileiro.

Falando em Estado Democrático de Direito, vem o princípio da dignidade da pessoa humana, que está na mira dos avanços tecnológicos, diante de ameaças como viés algorítmico e a automatização de processos. Imagine um robô julgando como uma calculadora, decisões jurídicas como alimentos, guarda, repartição de bens, divórcio litigioso, crimes e outras lides. Seria uma transferência do poder-dever do Estado de aplicar seu poder jurisdicional aos processos judiciais que são por natureza, complexas, à um robô inanimado e desumano que dá a palavra final, conforme o pensamento de Ferreira Filho (2023).

7. CONSIDERAÇÕES ÉTICAS E DESAFIOS

A Inteligência Artificial no Poder Judiciário enfrenta desafios como a prevenção de viés algorítmico, que pode perpetuar injustiças. A transparência é vital para garantir que todos compreendam como as decisões são tomadas.

O princípio da publicidade, como estabelecido no art. 93 da Constituição Federal deve ser o Norte para a implementação da IA. Qualquer inovação deve garantir a supervisão social e a possibilidade de contestação.

A obscuridade de alguns modelos de aprendizado de máquina (machine learning) pode tornar difícil para os profissionais de direito entenderem como uma decisão foi alcançada. Isso pode aventar preocupações sobre a transparência dos algoritmos de IA. Os sistemas de IA usados no sistema jurídico devem ser capazes de explicar de forma clara e compreensível como

chegaram a uma determinada conclusão. A falta de transparência pode acabar minando a confiança no sistema jurídico. (Negreiro, 2023).

Também é necessária a adoção de mecanismos claros de **accountability** (controle), com a inclusão de supervisão humana, é fundamental para assegurar que a Inteligência Artificial no Poder Judiciário seja empregada de forma ética e justa. Somente por meio dessas medidas de cautela, poderemos garantir que as inovações tecnológicas sirvam para promover um sistema de justiça mais equitativo, transparente e eficiente, sem renunciar aos valores fundamentais que sustentam o Estado Democrático de Direito, conforme Martins (2024).

Segundo Negreiro (2023), a responsabilidade legal é premente quando decisões são tomadas com base em algoritmos de IA. Quem é responsável, caso uma decisão automatizada se provar injusta ou prejudicial? Isso pode incluir decisões judiciais, recomendações legais ou pareceres jurídicos gerados por sistemas de IA. Definir a responsabilidade legal em tais casos é crucial para garantir a justiça e a prestação de contas.

8. GARANTIA DA PRIVACIDADE

A preocupação com a privacidade é fundamental. A Lei Geral de Proteção de Dados (LGPD), em vigor desde 2020, estabelece diretrizes claras sobre o tratamento dos dados pessoais, o que impacta diretamente a utilização da IA no Judiciário. O art. 7º da LGPD, por exemplo, fala sobre a necessidade de consentimento para o uso de dados pessoais, um aspecto vital que o Judiciário deve observar.

Negreiro (2023) diz que a coleta e o uso de dados pessoais são inerentes ao funcionamento da Inteligência Artificial. O Poder Judiciário deve garantir a privacidade e a segurança desses dados pessoais que é essencial. Os sistemas de IA no mundo jurídico precisam aderir a rigorosos padrões de proteção de dados para evitar violações de privacidade e vazamentos de informações confidenciais.

9. REGULAÇÃO E SUPERVISÃO

À medida que a IA continua a ser empregada no Direito, há uma crescente necessidade de regulação e supervisão adequadas. Os órgãos de regulação e as organizações profissionais devem trabalhar juntos para desenvolver diretrizes e padrões que governem o uso de IA na prática jurídica, para garantir que os profissionais do direito usem a tecnologia de maneira

responsável e ética. Isso pode incluir a criação de protocolos de certificação para ferramentas e sistemas de Inteligência Artificial, bem como a implementação de protocolos para determinar a responsabilização com intuito de garantir que os profissionais do direito cumpram as normas estabelecidas, segundo Oliveira (2022).

10. CONSIDERAÇÕES FINAIS E SUGESTÕES

Com as novas tecnologias de aprendizado de máquina, espera-se que assistentes virtuais consigam auxiliar na pesquisa de jurisprudência. A evolução da IA promete ser um grande aliado para advogados, juízes e cidadãos, mas a necessidade de regulamentação e supervisão ética continua sendo um ponto crucial.

A adoção da Inteligência Artificial no Judiciário brasileiro é uma oportunidade para promover a eficiência e a justiça. Entretanto, é crucial que essa implementação seja acompanhada por uma regulação rigorosa e por diretrizes claras. Algumas sugestões incluem:

- Desenvolvimento de Políticas Públicas: Criar políticas que orientem o uso da IA no Judiciário, assegurando que os direitos dos cidadãos sejam respeitados.
- Transparência e Controle: Implementar mecanismos de transparência e controle para as decisões automatizadas, permitindo auditorias regulares e supervisão dos algoritmos utilizados.
- Capacitação de Profissionais: Investir em programas de capacitação para juízes, advogados e servidores do Judiciário, assegurando que todos compreendam as implicações do uso da IA.
- Fomento à Pesquisa: Incentivar pesquisas sobre as implicações éticas e sociais do uso da IA no Judiciário, buscando soluções inovadoras para os desafios identificados.

11. CONCLUSÃO

A inteligência artificial representa uma ferramenta inovadora que pode transformar o Judiciário brasileiro, tornando-o mais eficiente e acessível. No entanto, a implementação dessa tecnologia deve ser cuidadosa e acompanhada por um forte arcabouço regulatório que garanta a proteção dos direitos fundamentais. A prevenção do viés algorítmico, a transparência nas decisões e a supervisão adequada são essenciais para assegurar que a justiça não seja apenas automatizada, mas também humanizada.

O futuro do Judiciário brasileiro dependerá de um diálogo constante entre tecnologia e direitos humanos, com a inclusão de todos os atores do sistema judicial, assegurando que a inovação não comprometa os pilares da justiça. O desenvolvimento de projetos como o Projeto

Victor do STF e a análise das experiências internacionais, como o ROSS nos EUA e os sistemas da Australia e do Reino Unido, são essenciais para a construção de um Judiciário mais ágil e justo.

A inteligência artificial possui o potencial de ser uma aliada crucial no aprimoramento do Poder Judiciário Brasileiro, promovendo maior eficiência, precisão e acesso à justiça. Contudo, a adoção consciente e ética dessa tecnologia é fundamental para garantir que não se percam os valores humanos e as garantias constitucionais.

REFERÊNCIAS

ALVES, Ítalo Miqueias S**. Os Impactos da Inteligência Artificial no Processo Jurídico Constitutivo do Direito Pós-Moderno**. Portal Âmbito Jurídico. Disponível em: https://ambitojuridico.com.br/os-impactos-da-inteligencia-artificial-no-processo-juridico-constitutivo-do-direito-pos-moderno/, 2022. Acesso em: 20 de outubro de 2024, 22:31.

BUOLAMWINI, Joy; GEBRU, Timnit. **Gender Shades:** Intersectional Accuracy Disparities in Commercial Gender Classification. Proceedings of Machine Learning Research, v. 81, 2018.

CASTRO JUNIOR, Antônio Pires, et al. **Aplicação da inteligência artificial na identificação e classificação automática de Incidente de Resolução de Demanda Repetitiva no Tribunal de justiça do Brasil**. Disponível em: https://revistas.ufg.br/revfd/article/view/70086, 2022. Acesso em: 20 de outubro de 2024, 22:33.

CONSELHO NACIONAL DE JUSTIÇA (CNJ)**. Democratizando o acesso à Justiça: 2022 / Conselho Nacional de Justiça**; Flávia Moreira Guimarães Pessoa, organizadora. – Brasília: CNJ, 2022. Disponível em: https://www.cnj.jus.br/wp-content/uploads/2022/02/democratizando-acesso-justica-2022-v2-01022022.pdf, 2022. Acesso em: 20 de outubro de 2024, 22:40.

CONSELHO NACIONAL DE JUSTIÇA (CNJ). **Ferramenta de IA vai auxiliar juízes fluminenses na elaboração de minutas de sentença**. Agência CNJ de Notícias. Disponível em: https://www.cnj.jus.br/ferramenta-de-ia-vai-auxiliar-juizes-fluminenses-na-elaboracao-de-minutas-de-sentenca/, 2024. Acesso em: 20 de outubro de 2024, 22:35.

CONSELHO NACIONAL DE JUSTIÇA (CNJ). **Justiça 4.0: Inteligência Artificial está presente na maioria dos tribunais brasileiros**. Agência CNJ de Notícias. Disponível em: https://www.cnj.jus.br/justica-4-0-inteligencia-artificial-esta-presente-na-maioria-dos-tribunais-brasileiros/, 2022. Acesso em: 20 de outubro de 2024, 22:39.

CONSELHO NACIONAL DE JUSTIÇA (CNJ). **Pesquisa revela que 47 tribunais já investem em inteligência artificial**. Agência CNJ de Notícias. Disponível em:

https://www.cnj.jus.br/pesquisa-revela-que-47-tribunais-ja-investem-em-inteligencia-artificial/, 2021. Acesso em: 20 de outubro de 2024, 22:29.

CONSELHO NACIONAL DE JUSTIÇA (CNJ). **Portal do Processo Judicial Eletrônico (PJe)**. Disponível em: https://www.cnj.jus.br/programas-e-acoes/processo-judicial-eletronico-pje/. Acesso em: 20 de outubro de 2024, 22:30.

CONSELHO NACIONAL DE JUSTIÇA (CNJ). **Uso de IA no Judiciário cresceu 26% em relação a 2022, aponta pesquisa.** Agência CNJ de Notícias. Disponível em: https://www.cnj.jus.br/uso-de-ia-no-judiciario-cresceu-26-em-relacao-a-2022-aponta-pesquisa/, 2024. Acesso em: 20 de outubro de 2024, 22:35.

FERREIRA FILHO, Moacir. **A Desumanização Do Direito: Uma Abordagem Acerca Do Uso Da Tecnologia No Ambiente Jurídico**. Disponível em: https://publicacoes.uniesp.edu.br/index.php/1/article/download/121/103/386, 2023. Acesso em: 20 de outubro de 2024, 22:23.

MARTINS, Daniel Carvalho. **Fundamentação das decisões e uso responsável de IA generativa no Judiciário**. Portal Consultor Jurídico. Disponível em: https://www.conjur.com.br/2024-ago-31/fundamentacao-das-decisoes-e-uso-responsavel-de-ia-generativa-no-judiciario/, 2024. Acesso em: 20 de outubro de 2024, 22:37.

MITCHELL, Tom M. **Machine Learning**. 1st ed. New York: McGraw-Hill, 1997.

NEGREIRO, Patrícia**. Aplicação da Inteligência Artificial no Mundo Jurídico: Vantagens, Desvantagens e Impacto**. Portal JusBrasil. Disponível em: https://www.jusbrasil.com.br/artigos/aplicacao-da-inteligencia-artificial-no-mundo-juridico-vantagens-desvantagens-e-impacto/1995452599, 2023. Acesso em: 20 de outubro de 2024, 22:32.

OLINDA, Érica Militão; CARVALHO, Larissa Fontenelle. **Accordes - fortalecendo o sistema de precedentes do STJ.** Portal EnAJUS. Disponível em: https://enajus.org.br/anais/assets/papers/2022/sessao-02/accordes-fortalecendo-o-sistema-de-precedentes-do-stj.pdf, 2022. Acesso em: 20 de outubro de 2024, 22:23.

OLIVEIRA, Antonildo. **Impacto da Inteligência Artificial no Direito: Desafios e Possibilidades**. Portal JusBrasil. Disponível em: https://www.jusbrasil.com.br/artigos/impacto-da-inteligencia-artificial-no-direito-desafios-e-possibilidades/1785412945, 2022. Acesso em: 20 de outubro de 2024, 22:31

RUSSELL, Stuart; NORVIG, Peter. **Artificial Intelligence: A Modern Approach.** 4th ed. Upper Saddle River: Pearson, 2021.

SIEGEL, Eric. **Predictive analytics: the power to predict who will click, buy, lie, or die**. Hoboken: Wiley, 2013.

SCHUCHOWSKY, Tatiana. **O Uso da Inteligência Artificial no Direito: Benefícios e Perspectivas**. Portal JusBrasil. Disponível em: https://www.jusbrasil.com.br/artigos/o-uso-da-inteligencia-artificial-no-direito-beneficios-e-perspectivas/2260063904, 2024. Acesso em: 20 de outubro de 2024, 22:38

SUPREMO TRIBUNAL FEDERAL (STF)**. Projeto Victor avança em pesquisa e desenvolvimento para identificação dos temas de repercussão geral**. Disponível em: https://noticias.stf.jus.br/postsnoticias/projeto-victor-avanca-em-pesquisa-e-desenvolvimento-para-identificacao-dos-temas-de-repercussao-geral/, 2021. Acesso em: 20 de outubro de 2024, 22:21.

TRAVIZANI, Apoliana Carriço, et al**. Uso da Inteligência Artificial no Poder Judiciário e os impactos no devido processo legal**. Portal Âmbito Jurídico. Disponível em: https://ambitojuridico.com.br/uso-da-inteligencia-artificial-no-poder-judiciario-e-os-impactos-no-devido-processo-legal/, 2021. Acesso em: 20 de outubro de 2024, 22:40.

TRIBUNAL DE JUSTIÇA DE MINAS GERAIS (TJ-MG)**. TJMG apresenta SOFIA: sistema de inteligência artificial em linguagem simples**. Disponível em: https://www.tjmg.jus.br/portal-tjmg/noticias/tjmg-apresenta-sofia-sistema-de-inteligencia-artificial-em-linguagem-simples.htm, 2023. Acesso em 20 de outubro de 2024, 22:39.

TRIBUNAL DE JUSTIÇA DE MINAS GERAIS (TJ-MG)**. TJMG utiliza inteligência artificial em julgamento virtual**. Disponível em: https://www.tjmg.jus.br/portal-tjmg/noticias/tjmg-utiliza-inteligencia-artificial-em-julgamento-virtual.htm, 2018. Acesso em: 20 de outubro de 2024, 22:35.

7 Information Society and Law
FMU CENTRO UNIVERSITÁRIO

A RACIONALIZAÇÃO FORMAL E BUROCRÁTICA ATRAVÉS DOS MECANISMOS DE INTELIGÊNCIA ARTIFICIAL DO PODER JUDICIÁRIO BRASILEIRO

FORMAL AND BUREAUCRATIC RATIONALIZATION THROUGH ARTIFICIAL INTELLIGENCE MECHANISMS OF THE BRAZILIAN JUDICIARY

Autor: Gustavo Rubio Claret Pereira[1]

Resumo: O presente resumo expandido[2] pretende analisar o inserimento das IA's (generativas ou não) no contexto do Poder Judiciário, compreendendo que este movimento de incorporação muito se adequa aos conceitos da sociologia de Max Weber, em especial, da burocratização e do racionalismo formal ou técnico. Como metodologia ao pretendido, este estudo busca relacionar pontos relevantes do estudo realizado pelo Painel da Pesquisa sobre Inteligência Artificial realizada em 2023 pelo Conselho Nacional de Justiça (CNJ) e a literatura corrente.
Palavras-Chave: Racionalismo formal; Burocracia; Judiciário; Max Weber, IA.

Abstract: This expanded abstract aims to analyze the integration of AI (both generative and non-generative) within the context of the Judiciary, understanding that this incorporation aligns closely with Max Weber's sociological concepts, particularly bureaucratization and formal or technical rationalism. As a methodology, this study seeks to relate key points from the research conducted by the National Council of Justice (CNJ) in 2023, named Artificial Intelligence Research Panel, linking to the current literature.
Keywords: Formal Rationalism; Burocracy; Judiciary; Max Weber; AI.

[1] Cientista Social formado pela Universidade de São Paulo (USP) e Bacharelando em Direito pela Faculdades Metropolitanas Unidas (FMU).
[2] O presente trabalho buscou rememorar os conceitos sociológicos de Max Weber ante a matéria jurídica processual desempenhada pelos Tribunais de Justiça brasileiros com o advento dos mecanismos de Inteligência Artificial.

> "Um algoritmo é uma sequência de instruções que informa ao computador o que ele deve fazer. Os computadores são compostos por bilhões de minúsculas chaves chamadas transistores, e os algoritmos ligam e desligam essas chaves bilhões de vezes por segundo. O algoritmo mais simples é: gire a chave. O estado de um transistor contém um único bit de informação: um, se o transistor estiver ativado, e zero, se estiver desativado. Um único bit em algum local dos computadores de um banco informa se nossa conta tem ou não saldo. Outro bit dos computadores da administração da previdência social informa se estamos vivos ou mortos. O segundo algoritmo mais simples é: combine dois bits. Claude Shannon, conhecido como o pai da teoria da informação, foi a primeira pessoa a entender que o que os transistores fazem, quando ligam e desligam em resposta a outros transistores, chama-se raciocínio (...)" (Domingos, 2017, p. 20).

> "A burocratização é provocada mais pelo aumento intensivo e qualitativo e o desenvolvimento interno das tarefas administrativas que pela ampliação extensiva e quantitativa. Mas há uma grande variação na direção tomada pela burocratização e os motivos que a provocam. (Weber, 2014, p. 33).

INTRODUÇÃO

O escopo que se pretende neste trabalho, especialmente atento ao tema que compõe Inteligência Artificial e Poder Judiciário, busca analisar os aspectos sociológicos que refletem sobre como o inserimento das tecnologias, ferramentas e o advento da Inteligência Artificial impactam e geram no imaginário social e jurídico a ideia de que a "era da tecnologia" resultará no fim das estruturas burocráticas.

Para tanto, analisa comparativamente os mecanismos de Inteligência Artificial mobilizados pelo Judiciário, especialmente aqueles mencionados pelo Painel da Pesquisa sobre Inteligência Artificial realizada em 2023 pelo Conselho Nacional de Justiça (CNJ) e legislação aos conceitos da literatura sociológica weberiana relativos à racionalização formal e formas burocráticas.

DISCUSSÕES E RESULTADOS

Nada obstante os riscos postos pela "evolução tecnológica" que se refere, a pretensão deste trabalho é tratar de compreender a dimensão mais razoável dos algoritmos, pelo que verdadeiramente são, nada mais que ferramentas. E mesmo no convívio da plena automatização, com o surgimento de boots (robôs), com toda essa aparência mais bem acabada, todos estes mecanismos tecnológicos trata-se apenas de novas ferramentas, técnicas e artifícios, contudo, sempre mais sofisticado que o anterior.

Posto estes esclarecimentos necessários, retoma-se ao conceito de burocracia estabelecido por Max Weber, visto que a noções delineadas por este grande expoente da sociologia ainda perseveram e estabelece diálogo com os princípios jurídicos da administração pública brasileira. De início, Weber analisa e concebe a máquina burocrática pelo princípio da Hierarquia, que garante a operação de um sistema de normas assegurando a execução e preservação de direitos e deveres. A relevância da "modelização" proposta por Weber da máquina burocrática permanece corrente, sobretudo pela acurácia de sua terminologia.

A burocratização, tendência técnica/sociológica exposta por Weber, avança socio temporalmente às demais sociedades do globo, é parte de sua teoria maior, a noção de desencantamento do mundo. Dela se abstrai que a globalização se dará continuamente através de uma constante racionalização e conceituação, com intuito de universalização.

Como apontado pelo sociólogo Gabriel Cohn, o centro de análise de Weber quanto ao tema do poder se deve à compreensão de como se dá sua legitimação. O engendramento do poder pela máquina estatal ocorre pela conformação da estrutura burocrática, que nada mais é do que uma racionalização. Sendo a estrutura burocrática, portanto, um modus de operacionalização e de legitimação. (COHN: 2009).

Há que se distinguir dentre os conceitos que a compreensão da racionalização formal e técnica é típica da máquina estatal que compõem o que chamamos de burocracia, enquanto a racionalização substantiva remete a compreensão da teoria maior e sociológica do autor – neste sentido, mais amplo, a racionalização (substantiva) remete ao quadro valorativo que orienta as ações dos indivíduos em sociedade.

A racionalização, portanto, pode se referir tanto a um processo de estruturação e aperfeiçoamento do poder pela estrutura estatal, em legitimação do poder, quanto ao conjunto de valores (ideologias) que guiam os indivíduos para determinada ação social, compreendendo, assim, um arcabouço sociológico possível. (THIRY-CHERQUES: 2009).

Feitas as distinções entre a racionalização formal e substantiva, sendo a primeira de maior relevância para o caso em comento, há que se compreender, portanto que o procedimento de burocratização é um fenômeno que Weber suscita existir ao longo da história das sociedades, que encontra nas sociedades modernas a sua forma mais bem acabada. Relembrando as pontuações de Cohn sobre os desígnios do autor, retoma-se a

questão sobre a legitimação do poder, sendo que possível ocorrer por duas vias, primeiramente pela violência, e em segundo lugar, pela legitimação burocrática.

Neste sentido, a burocracia é apenas um recorte da face mais bem acabada das estruturas sociais, que se consolidam e engendram-se em aparato estatal ou paraestatal (direito privado). Tal como Marx, Weber era grande estudioso da história comparativa, e como resquício de uma época, refletia sua teoria sobre modelos históricos que pendiam para uma concepção histórica evolutiva.

Retomando ao contexto atual, ao momento dos adventos tecnológicos em diversas escalas e subsumindo os modelo teórico proposto por Weber à administração pública brasileira, faz-se mister compreender às inovações recém inseridas no Poder Judiciário, com base no Painel da Pesquisa sobre Inteligência Artificial 2023, estudo encomendado pelo Ministro realizado pelo Conselho Nacional de Justiça envolvendo 94 órgãos do Poder Judiciário, que contabilizou ao menos 140 projetos de IA desenvolvidos e postos à disposição dos tribunais e conselhos de Justiça.

Dentre as atividades trabalhadas por estes projetos, estão as buscas por casos similares, classificação de documentos, padronização de jurisprudência, sugestão de movimentos para despacho e até mesmo a elaboração de ementas, apenas citando algumas das atividades. Em suma, ainda não se objetiva no Poder Judiciário projetos de IA generativa, mesmo que certos projetos mencionados enveredem muito próximo do ramo das *Machines Learnigs*. No entanto, é possível antever que os robôs postos à disposição do Judiciário estão assumindo cada vez mais cargas de treinamento, enriquecidos com informações mais densas e, respectivamente, operacionalizando mais algoritmos que nunca.

Este limite tênue, inclusive, ensejou a disposição da Resolução do CNJ nº 332, de 21/08/2020, que estabeleceu limites a atuação e aplicação da Inteligência Artificial, sobretudo quanto as práticas discriminatórias e ao respeito do direitos fundamentais, prevendo o controle através do CNJ, através de recurso denominado SINAPSE, que segundo a definição disposta no inciso III, do Art. 3º desta resolução, se trata de: "*solução computacional, mantida pelo Conselho Nacional de Justiça, com o objetivo de armazenar, testar, treinar, distribuir e auditar modelos de Inteligência Artificial"* (DJe/CNJ, nº 274, de 25/08/2020, p. 4-8).

A racionalização formal, tal como a comentada inicialmente sobre a terminologia weberiana, estrutura a máquina burocrática e têm hoje seu ápice com a aplicação dos projetos

de IA para a solução e eficiência dos processos judiciais. As novas tecnologias não são ponto de ruptura da norma e da formalização dos procedimentos e técnicas da burocracia, mas o seu oposto, isto é, uma maior concentração dos instrumentos burocráticos em contato multidisciplinar de áreas da tecnologia.

Como resultado do encontro entre tecnologia e a burocracia, prevalece a regra da normatividade e da hierarquia, esta última exercida pelo Poder Judiciário, como a relação disposta em redação da Resolução, que prevê diversas vezes no texto legal a submissão dos projetos de IA ao controle do CNJ. Controle que ocorre também através de outro sistema de IA.

Os novos mecanismos, que se sucedem uns aos outros, acumulam novas competências ou aperfeiçoamentos e, ainda assim, submetem-se aos limites e forma cogente prevista na resolução. Curiosamente, este rigor atrela a tecnologia e burocracia em um ciclo contínuo, e sob esta perspectiva não haveria razão de operacionalização das novas tecnologias se estas não ocorressem sob etapas da estrutura burocrática.

A redução da burocracia digital através dos sistemas de IA, incorporados pelos Tribunais de Justiça, demonstra ser o propósito majoritário dentre os projetos pinçados pelo estudo do CNJ, a disposição da técnica mais racional no contexto do algoritmo buscou reduzir a extensividade do que antes se estabelecia em um contexto analógico.

Ao passo que a IA generativa, que possui alto grau de autonomia e capaz de produzir novos conteúdos utilizando-se de um vasto banco de dados e que atualmente têm provocado reações antagônicas, sejam pelo seu apelo ou pelo risco de manipulação e diretrizes confiáveis, não compõem os projetos listados pelo CNJ. Contudo, ao mencionar a IA generativa percebe-se que a Resolução nº 332/20 anteviu os riscos e estabeleceu limites para os projetos, sobretudo em relação as distorções que eventualmente poderiam ocorrer através de sua implementação. Ao disciplinar em seu capítulo III, “da não discriminação”, a obrigatória vistoria dos projetos implementados e se estão em concordância aos direitos fundamentais, nota-se a preocupação especial quanto aos possíveis preconceitos ou generalizações que porventura possam ter sido introduzidos ao longo do desenvolvimento do projeto.

Também, prevê a Resolução nº 332/20 que ao momento da implementação de modelos de IA, estes deverão utilizar-se preferencialmente softwares com código aberto, facilitando a integração e cooperação aos sistemas utilizados pelo sistema judiciário, além de proporcionar maior transparência da sua aplicação e desenvolvimento.

De certo modo, evidencia-se a compreensão do Poder Judiciário da dinâmica da técnica formal e da constante racionalização através da inteligência artificial, dispondo com cautela sobre questões que ainda não estão plenamente estabelecidas. Justamente ao compreender-se que o avanço tecnológico não é em sua essência incompatível com a razão burocrática, é composição deste processo de desencantamento e racionalização cada vez mais acelerada que envolve também a máquina pública.

Parafraseando Pedro Domingos, especialista versado em *Machine Learning*, cuja especialidade de IA generativa e autônoma é conhecida por gerar soluções através do aprendizado contínuo das padronizações de algoritmos – não é razoável mantê-las em "caixas pretas", pois o desconhecimento da sua envergadura apenas dá entrada para o uso incorreto e para o erro grosseiro (DOMINGOS: 2017). Em razão disso, como comentado acima, CNJ previu em resolução como prioridade a implementação de projetos de IA com código aberto, a fim de que estes possam ser revisados e melhorados, também contribuindo para maior transparência destes mecanismos.

CONCLUSÃO

Por fim, analisando o contexto do Poder Judiciário frente as inúmeras ferramentas de IA à disposição, sejam elas generativas ou não, nota-se que a utilização destas tecnologias, por mais autônomas que possam parecer, seja na elaboração integral de despachos, ementas ou quaisquer outros atos específicos, não resultariam no esvaziamento da capacidade de poder das autoridades judiciária, justamente por entender que mesmo nestas situações seriam necessárias padronização, ratificação e decisão destes agentes.

Por outro lado, ao supor que muito em breve a elaboração sucessiva de atos judiciais via inteligência generativa se torne regularidade, há que se questionar se estes "atos", produzidos de maneira impessoal, certamente embasados em padrões e orientações das corregedorias e conselhos respectivos, não imprimiriam maior regularidade e eficiência e celeridade à jurisprudência vindoura, questão que se abre para reflexão.

REFERÊNCIAS

COHN, Gabriel. Max Weber: Muito além do Estado nacional. *In*: ALMEIDA, Jorge de; BADER, Wolfgang: **Pensamento alemão no século XX**: grandes protagonistas e recepção das obras no Brasil. São Paulo: Cosac Naify, 2009.

DOMINGOS, Pedro. **O algoritmo mestre**: como a busca pelo algoritmo de machine learning definitivo recriará nosso mundo. São Paulo: Editora Novatec, 2017.

THIRY-CHERQUES, Hermano Roberto. Max Weber: o processo de racionalização e o desencantamento do trabalho nas organizações contemporâneas. **Revista de Administração Pública**. RAP – Rio de Janeiro 43(4): 897-918, JUL/AGO 2009.

WEBER, Max. "Burocracia". In: WEBER, Max: **Ensaios de Sociologia**. 5. ed. Rio de Janeiro: LTC, 1999. Cap. 8. p. 229-282.

WEBER, Max. **Economia y Sociedad**. México: Fondo de Cultura Económica, 1964.

PAINEL DA PESQUISA SOBRE INTELIGÊNCIA ARTIFICIAL 2023 – CONSELHO NACIONAL DE JUSTIÇA: Disponível em: https://paineisanalytics.cnj.jus.br/single/?appid=43bd4f8a-3c8f-49e7-931f-52b789b933c4&sheet=53cb7211-d465-4ee7-ad18-e57c7f50085b&theme=horizon&lang=pt-BR&opt=ctxmenu,currsel&select=Ramo%20da%20Justi%C3%A7a,&select=Tribunal,&select=Seu%20Tribunal/%20Conselho%20possui%20Projeto%20de%20IA.

Resolução n° 332 de 21/08/202 do Conselho Nacional de Justiça (CNJ), publicada no DJe/CNJ, nº 274, de 25/08/2020, p. 4-8. Disponível em: https://atos.cnj.jus.br/atos/detalhar/3429.

7 Information Society and Law
FMU CENTRO UNIVERSITÁRIO

A INTELIGÊNCIA ARTIFICIAL E OS ALGORITMOS NO PODER JUDICIÁRIO

ARTIFICIAL INTELLIGENCE AND ALGORITHMS IN THE JUDICIARY

Luiz Eduardo Alves de Siqueira[1]

Resumo: O presente trabalho objetiva, tomando por base a informatização, e, na sequência dela, o emprego da inteligência artificial (IA) destacar os benefícios, obstáculos e casos exemplares de seu emprego no Poder Judiciário brasileiro. A análise, para além disso, também perquire os prós e contras de tal inserção. A delimitação é dada tomando por base ações cíveis no Tribunal de Justiça do Estado de São Paulo (TJ-SP), no intervalo entre 2016 e 2026. A metodologia de pesquisa toma por base o método dedutivo, partindo-se da situação geral proporcionada pela introdução das IAs direcionando-se, em específico, para a prestação jurisdicional da Corte indicada. Suas técnicas consistirão em pesquisa bibliográfica, bem como contato direto com os mecanismos pertinentes não apenas com o TJ-SP, mas de outros tribunais que têm, ao longo do Brasil e mesmo do estrangeiro, empregado a inovação tecnológica em questão, apurando limitações e avanços proporcionados. Será utilizada combinação de pesquisa histórica e teórica, tanto na fase de investigação, quanto na fase de tratamento dos dados e, a depender do resultado das análises, nos relatórios de pesquisa poderá ser empregado outro método que for mais indicado. Os resultados, por ora, indicam para considerável melhoria na eficiência da aplicação da lei nos tribunais que puseram em execução a IA como uma instrumental de trabalho. O emprego da IA permite apreciação mais ágil e precisa de dados complexos, contribuindo para a aceleração da solução dos processos. Essa abordagem se alinha com os avanços tecnológicos, oferecendo soluções inovadoras para os desafios em constante evolução no sistema legal brasileiro. Por fim, nas possíveis críticas e sobretudo abusos ao funcionamento de tal mecanismo, propõe, já nos termos do preconizado pelo Projeto de Lei (PL) nº 21/2020, o uso do relatório de impacto da inteligência artificial como forma de transmitir transparência no uso de algoritmos, que são os meios pelos quais a IA se materializa.
Palavras-Chave: Poder Judiciário; Inteligência Artificial; algoritmos; efetividade jurisdicional.

Abstract: This paper aims to highlight the benefits, obstacles, and exemplary cases of the use of artificial intelligence (AI) in the Brazilian Judiciary, based on the process of digitization and, subsequently, the employment of AI. Moreover, the analysis also examines the pros and cons of such implementation. The focus is on civil actions within the São Paulo State Court of Justice (TJ-SP, acronym in Portuguese) between 2016 and 2026. The research methodology is based on the deductive method, starting from the general situation provided by the introduction of AI, specifically addressing the judicial services of the indicated Court. The techniques used include

[1] Possui graduação em Direito pela Universidade de São Paulo (1995), especialização em Direito Constitucional, mestrado (2008) e doutoramento (2015) em Integração da América Latina pela Universidade de São Paulo (Prolam). Professor do Mestrado em Direito da Sociedade da Informação das Faculdades Metropolitanas Unidas (FMU).

bibliographical research, as well as direct interaction with the relevant tools not only at the São Paulo State Court of Justice (TJ-SP), but also at other courts in Brazil and abroad that have adopted this technological innovation, investigating the limitations and advances provided. A combination of historical and theoretical research is used both in the investigation, and in the data analysis phase, and depending on the results, other methods may be employed in the research reports if deemed more appropriate.
So far, the results indicate a significant improvement in the efficiency of law enforcement in courts that have implemented AI as a working tool. The use of AI allows for quicker and more accurate processing of complex data, contributing to faster resolution of cases. This approach aligns with technological advances, offering innovative solutions to the constantly evolving challenges of the Brazilian legal system. Finally, regarding potential criticisms and especially abuses in the operation of such tool, it proposes, as stated by Bill (PL, acronym in Portuguese) No. 21/2020, the use of an artificial intelligence impact report to ensure transparency in the use of algorithms, which are the means by which AI is implemented.
Keywords: Judiciary; Artificial Intelligence; algorithms; jurisdictional effectiveness.

INTRODUÇÃO

O estágio atual das ciências, em particular da engenharia, da informática e da robótica, permitiu o desenvolvimento de algoritmos inteligentes capazes, em princípio, de reproduzirem alguns comportamentos tipicamente humanos. Assim, considerando que o objetivo dos desenvolvedores dessa tecnologia é a utilização de tais algoritmos em larga escala, especialmente, mas não se limitando, ao desenvolvimento de máquinas autônomas a serem aplicadas em vários setores, e, no particular, ao Poder Judiciário, mormente quando colocada a questão em face da complexidade e dinamismo das relações jurídicas que, indubitavelmente, submete as pessoas a um processo constante de tomada de decisões; e, por derradeiro, considerando os riscos às pessoas naturais e/ou jurídicas daí advindos, coloca-se ao Direito a necessidade imediata de tomada de posição, visando a adequar alguns de seus institutos a essa nova realidade formatada pela tecnologia.

Nessas condições, como o Poder Judiciário, ao se valer da IA, compete investigar, coloca a celeridade na prestação jurisdicional em detrimento dos direitos humanos fundamentais dos jurisdicionados? O relatório de impacto de inteligência artificial poderia, ainda que a matéria seja de lege ferenda, pôr cobro a eventuais abusos, à medida que se destina, no dizer do artigo 2º, inciso VI, do PL nº 21/20, "a documentação dos agentes de inteligência artificial que contém a descrição do ciclo de vida do sistema de inteligência artificial, bem como medidas, salvaguardas e mecanismos de gerenciamento e mitigação dos riscos relacionados a cada fase do sistema, incluindo segurança e privacidade". (g.n.)

A partir daí, considerando que hipóteses são possíveis respostas ao problema de pesquisa lançado, segundo Orides Mezzarobba (2009, p. 152), esperou-se, mediante a pesquisa, identificar que o uso das IAs agiliza, por um lado, a prestação jurisdicional, mas, por outro, permite, enquanto não regulamentados os meios de controle do uso de algoritmos, possíveis violações a direitos humanos fundamentais, entre os quais o de personalidade, e do próprio acesso efetivo à jurisdição.

O presente trabalho empregou como o método dedutivo como metodologia, partindo-se da situação geral proporcionada pela introdução das IAs, direcionando-se, em específico, para a prestação jurisdicional da Corte indicada. As técnicas levaram em conta julgados, documentos oficiais e textos doutrinários a respeito da situação.

Cabe, antes de apresentar a base teórica que deu lastro ao estudo em comento, historiar que o avanço tecnológico no Poder Judiciário brasileiro, com o emprego de novas ferramentas de IA, teve lugar porque consequência do cenário formado pelo advento da Sociedade da Informação e da denominada 4ª Revolução Industrial.

Assim, invocando Manuel Castells (2003, passim), que Sociedade da Informação (SI) é a sociedade tecnológica surgida ao término do século passado, como reflexo da sociedade pós-industrial, marcada pela informação como matéria-prima, emprego acelerado das redes e o relacionamento interpessoal acentuado em virtude delas, o capitalismo de plataforma, o que enseja, assim, desdobramentos políticos, sociais e jurídicos. O comportamento da humanidade, na SI, já se apresenta diferenciado, e o aproveitamento no Poder Judiciário revelou-se inevitável.

Esse período histórico é denominado, também, de 4ª Revolução Industrial, sendo desse modo identificada:

> Vivemos um momento especial que se convenciona denominar Quarta Revolução Industrial. Nesses tempos estranhos, a tecnologia vem mudando rapidamente a sociedade em que vivemos. São três os fatores que respondem pela maior parte dessa mudança: aumento exponencial da capacidade computacional, a difusão de técnicas de inteligência artificial, e o advento do big data (FERRARI, 2021, p. 09).

Indo a seguir, dentro do processo de informatização acentuado trazido pela SI veio a IA, que pode ser definida como o conjunto de tecnologias, concebida já na década de 1950, mas apenas mais recentemente possibilitada para emprego em maior incidência. A expansão do uso da IA em variados setores da vida humana ocorreu em razão da transformação digital que disponibilizou um volume enorme de dados, chamado de big data, que formam a

base da IA, além dos desenvolvimentos de capacidades cognitivas artificiais e de novos algoritmos de aprendizagem, chamados de machine learning (MITTELSTADT, 2016).

Inteligência Artificial é um sistema digital capaz de obter e produzir resultados de maneira ilimitada e independente, imitando e emulando a inteligência humana, isto é, ser capaz de pensar como pensa o cérebro humano, criando soluções novas, mas sempre artificialmente. Magrini assim a define: "A inteligência artificial é um subcampo da informática. Seu objetivo é habilitar o desenvolvimento de computadores que sejam capazes de emular a inteligência humana ao realizar determinadas tarefas" (2019, p. 51).

A IA é composta pelos seguintes elementos: software, hardware, base de dados (big data) e algoritmos (machine learning). O software é o programa de computador que determina o procedimento a ser seguido. O hardware é a base física do sistema de IA. O algoritmo é uma construção matemática antiga usada para processar dados que produzem evidências e motivam ações específicas em direção à solução de determinado problema. Nesse sentido, um algoritmo vai além de uma sequência de passos precisos para a efetivação de uma tarefa, porque envolve atores autômatos ou seres humanos na tomada de decisão automatizadas ou na repetição de ações com o objetivo de processar um volume enorme de dados como se fosse uma receita de um bolo. O algoritmo é apenas um dos elementos da IA e exige proteção jurídica para o seu emprego e o resultado que dele advém.

Sendo o seu emprego uma constante, sobretudo no sistema financeiro, terminou por atrair a atenção do Poder Judiciário, que, se principiou há cerca de uma década a digitalização de autos, passou a seguir por regulamentar a novidade por intermédio da Resolução nº 332, do Conselho Nacional de Justiça, que a define:

> Art. 3º Para o disposto nesta Resolução, considera-se:
> (...)
> II – Modelo de Inteligência Artificial: conjunto de dados e algoritmos computacionais, concebidos a partir de modelos matemáticos, cujo objetivo é oferecer resultados inteligentes, associados ou comparáveis a determinados aspectos do pensamento, do saber ou da atividade humana;

É importante estabelecer distinção entre a IA e a automação e robotização, pois nessas os resultados são definidos anteriormente e parametrizados. Os algoritmos de aprendizagem, levados ao limite, podem redundar em tomadas de decisões imprevisíveis e incontroláveis, as quais podem, inclusive, propiciar incontáveis violações de direitos humanos.

Indo além, o Poder Judiciário partiu da automação para o suo de ferramentas de IA, tendo sido criados sistemas próprios nos Tribunais, como o Victor, no Supremo Tribunal Federal, Athos, Sócrates, E-juris e TUA, no Superior Tribunal de Justiça, Sinapses, do Conselho Nacional de Justiça, entre muitos outros. Eles funcionam não só para a automação de tarefas ordinárias como para subsidiar decisões judiciais humanas, promovendo a celeridade no processamento. Apenas para que se mencione uma delas, o já aludido sistema Victor permite transformar imagens em textos no processo digital, separar e classificar as peças processuais mais utilizadas nas atividades do Supremo Tribunal Federal, separar e classificar documentos, identificar temas de repercussão geral mais comuns e auxiliar na resolução dos recursos extraordinários.

De outro lado, meio que prevendo os riscos da automação, a Lei Geral de Proteção de Dados (LGPD), em seu artigo 20, já preconizava que:

> Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.
> § 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.
> § 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.

Inúmeros são riscos e desafios que surgem para o Direito na utilização de Inteligência Artificial e, principalmente, no uso de algoritmos no processo de tomada de decisão. As decisões tomadas por algoritmos decisórios trazem riscos referentes a: responsabilização pelos danos causados; opacidade pela falta de transparência dos motivos das decisões tomadas; efeitos discriminatórios.

Nessa toada, tramita pelo Congresso Nacional o Projeto Legislativo nº 20/2021, que objetiva regulamentar, dentro do que é possível, a IA. Um dos mecanismos, já previstos no art. 38 da LGPD, é o do relatório de impacto. A proposta em comento dele trata do relatório de impacto de inteligência artificial, conceituando-o em seu artigo 2º, inciso VI:

> relatório de impacto de inteligência artificial: documentação dos agentes de inteligência artificial que contém a descrição do ciclo de vida do sistema de inteligência artificial, bem como medidas, salvaguardas e mecanismos de gerenciamento e mitigação dos riscos relacionados a cada fase do sistema, incluindo segurança e privacidade.

Esse instrumento, frise-se, pode ser instrumento bastante interessante, mesmo considerando que, na "algoritimização", haja máquinas dialogando com máquinas, e, a despeito da programação havida, não se pode garantir que estejam sujeitas a rígido controle. Assim mesmo, o relatório vem ao encontro do que já fora preconizado na LGPD, não se verificando, ao menos por ora, seu emprego nos trabalhos do Tribunal mencionado.

O referencial teórico adotado, além do estudo comentado das normas apresentadas, levou em conta também o trabalho sobre Inteligência Artificial elaborado pelo Programa de Mestrado em Sociedade da Informação das Faculdades Metropolitanas Unidas, os autores Patrícia Peck Pinheiro, Bruno Bioni, Danilo Doneda, bem como as mais recentes publicações sobre o tema.

CONCLUSÃO

Por ora, sabe-se que a algoritmização tem sido levada a efeito pelo Tribunal de Justiça de São Paulo, e, embora agilize bastante o trabalho, não está a salvo, primeiro, de críticas por fomentar preconceitos, e, depois, porque, perigosamente, não pode, ao contrário do que se supõe, substituir o trabalho humano na prestação jurisdicional. Nesse aspecto, igualmente, a inexistência, até o momento, do relatório de impacto, não permite exercer controle sobre os algoritmos, que, por isso, se otimizam o trabalho, por outro podem dar margens a preconceitos de toda ordem, que culminam, no limite, com a má prestação jurisdicional. Os textos devem ser digitados em parágrafos. Desloca-se a primeira linha de cada parágrafo em 1,5 cm da margem esquerda. Requer-se a utilização de fonte Times Nem Roman, tamanho 12 para o texto, com espaçamento 1,5 de entrelinhas. As folhas devem apresentar margem esquerda e superior de 3 cm; direita e inferior de 2 cm.

REFERÊNCIAS

BARCAROLLO, Felipe. Inteligência artificial e a gramática ético-jurídica da sociedade (pós) -humana. Orientador: Wilson Engelmann. 308 f. Tese (Doutorado em Direito) – Programa de pós-graduação em Direito da Universidade do Vale do Rio dos Sinos UNISINOS, São Leopoldo, 2019. Disponível em: http://www.repositorio.jesuita.org.br/handle/UNISINOS/1647. Acesso em: 21 ago.2024.

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2021.

BRAGANÇA, Fernanda; BRAGANÇA, Laurinda Fátima da F.P.G. Revolução 4.0 no Poder Judiciário: Levantamento do uso de inteligência artificial nos tribunais brasileiros. **Revista da SJRJ**, Rio de Janeiro, v. 23, n. 46, p. 65-76, 22 11 2019. Disponível em: http://revistaauditorium.jfrj.jus.br/index.php/revistasjrj/article/view/256. Acesso em: 22 ago.2024.

BRASIL. Câmara dos Deputados**. Projeto de Lei nº 21/2020**. Estabelece princípios, direitos e deveres para o uso de inteligência artificial no Brasil, e dá outras providências. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2236340&fichaAmigavel=nao#:~:text=PL%2021%2F2020%20Inteiro%20teor,Projeto%20de%20Lei&text=Estabelece%20princ%C3%ADpios%2C%20direitos%20e%20deveres,Brasil%2C%20e%20d%C3%A1%20outras%20provid%C3%AAncias.&text=NOVA%20EMENTA%3A%20Estabelece%20fundamentos%2C%20princ%C3%ADpios,Brasil%3B%20e%20d%C3%A1%20outras%20provid%C3%AAncias. Acesso em: 23 ago.2024.

BRASIL. Conselho Nacional de Justiça**. Resolução nº 332**, de 21/08/2020. Dispõe sobre a ética, a transparência e a governança na produção e no uso de Inteligência Artificial no Poder Judiciário e dá outras providências. Disponível em: https://atos.cnj.jus.br/atos/detalhar/3429. Acesso em: 22 ago.2024.

BRASIL. **Lei nº 13.709**, de 14 de agosto de 2018. Lei Geral de Proteção de Dados. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 24 ago.2024.

CASTELLS, Manuel. **A galáxia da Internet**: reflexões sobre a internet, os negócios e a sociedade. Rio de Janeiro: Jorge Zahar, 2003.

COSTA, Ramon; KREMER, Bianca. Inteligência artificial e discriminação: desafios e perspectivas para a proteção de grupos vulneráveis diante das tecnologias de reconhecimento facial. **Direitos Fundamentais & Justiça**, Belo Horizonte, ano 16, p. 145-167, out. 2022. Número especial. Disponível em: https://doi.org/10.30899/dfj.v16i1.1316. Acesso em: 21 ago.2024.

DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

FERRARI, Isabela (coord.) **Justiça Digital**. São Paulo: Thomson Reuters Brasil, 2021.

MAGRINI, Eduardo. **Entre dados e robôs**: ética e privacidade na era da hiperconectividade. Porto Alegre: Arquipélago Editorial, 2019.

MCCARTHY, John et al. A proposal for the dartmouth summer research project on artificial intelligence, august 31, 1955. **AI magazine**, v. 27, n. 4, p. 12, 2006.

MEZZAROBA, Orides; MONTEIRO, Cláudia Servilha. **Manual de Metodologia da Pesquisa no Direito**. 5. ed. São Paulo: Saraiva, 2009.

MITTELSTADT, Brent Daniel; ALLO, Patrick Allo; TADDEO, Maria Rosaria; WACHTER, Sandra; FLORIDI, Luciano. The ethics of algorithms: Mapping the debate. **Big Data & Society**. July–December 2016: 1–21.

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

PROJETO VICTOR AVANÇA EM PESQUISA E DESENVOLVIMENTO PARA IDENTIFICAÇÃO DOS TEMAS DE REPERCUSSÃO GERAL. Portal STF. 19 de outubro de 2021. Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=471331&ori. Acesso em: 25 ago.2024.

RIBEIRO, Ricardo Silveira. Inteligência artificial, Direito e equidade algorítmica: discriminações sociais em modelos de machine learning para a tomada de decisão**. Revista de Informação Legislativa**: RIL, Brasília, DF, v. 59, n. 236, p. 29-53, out./dez. 2022. Disponível em: https://www12.senado.leg.br/ril/edicoes/59/236/ ril_v59_n236_p29. Acesso em: 24 ago.2024.

VIGLIAR, José Marcelo Menezes (org.). **Inteligência Artificial** (Obra coletiva). Almedina Brasil: São Paulo, 2023.

7 Information Society and Law
FMU CENTRO UNIVERSITÁRIO

USO DA INTELIGÊNCIA ARTIFICIAL NA FISCALIZAÇÃO TRIBUTÁRIA E SEUS EFEITOS SOBRE OS DIREITOS FUNDAMENTAIS

THE USE OF ARTIFICIAL INTELLIGENCE TAX INSPECTION AND ITS EFFECTS ON FUNDAMENTAL RIGHTS

Stefanie Cristine Kulkas da Silva[1]

Resumo: O presente estudo busca analisar a aplicação da Inteligência Artificial na fiscalização tributária no Estado Democrático de Direito. Por meio do método dedutivo, a partir de pesquisa legislativa e bibliográfica, o texto destaca a competência da Administração Pública, as previsões legais para atividade fiscalizatória e sua relevância para o funcionamento do Estado. Além disso, é enfatizado o uso do Sistema de Seleção Aduaneira por Aprendizado de Máquina (SISAM) como forma de aprimorar a fiscalização aduaneira, discutindo seus impactos quanto aos Direitos Fundamentais.
Palavras-Chave: Inteligência Artificial; Fiscalização Tributária; SISAM; Direitos Fundamentais.

Abstract: The present study seeks to analyze the application of Artificial Intelligence in tax inspection in the Democratic Rule of Law. Through the deductive method, based on legislative and bibliographic research, the text highlights the competence of the Public Administration, the legal provisions for inspection activity and its relevance to the functioning of the State. In addition, the use of the Machine Learning Customs Selection System (SISAM) is emphasized as a way to improve customs inspection, discussing its impacts on Fundamental Rights.
Keywords: Artificial Intelligence; Tax Inspection; SISAM; Fundamental Rights.

INTRODUÇÃO

A fiscalização tributária exerce papel fundamental para manutenção do funcionamento do Estado Democrático de Direito. O controle das atividades fiscais exercidas pelos contribuintes, com estrito respeito aos direitos fundamentais, constitui-se não somente numa forma de arrecadação para o Poder Público, mas também um mecanismo para identificação de irregularidades e ilegalidades com potencial risco à segurança pública.

Diante de sua relevância e dos constantes avanços tecnológicos da sociedade, o aprimoramento do processo fiscalizatório tornou-se uma preocupação constante para a

[1] Graduanda em Direito pela FMU - SP. Email: stefaniekulkas2805@gmail.com.

Administração Pública, que tem, dentre uma de suas principais atribuições, a atividade de polícia administrativa.

O advento da Inteligência Artificial e sua constante evolução passaram a representar uma oportunidade de melhoria para o controle fiscal, possibilitando a implementação de sistemas que tem por objetivo auxiliar o ser humano e tornar os processos mais céleres e eficazes, sem transferir o poder decisório à máquina.

Nesse contexto, a fiscalização aduaneira, enfatizada neste estudo, passou a utilizar o Sistema de Seleção Aduaneira por Aprendizado de Máquina (Sisam) como ferramenta para melhorar o processo de separação de mercadorias para os canais adequados, além de auxiliar na escolha de quais devem ser vistoriadas fisicamente por meio de métodos probabilísticos. Entretanto, é necessário considerar não somente os aspectos práticos relacionados ao seu uso, mas também os jurídicos e legais, principalmente no que concerne aos direitos fundamentais do contribuinte.

Assim, por meio do método dedutivo, a partir de pesquisa legislativa e bibliográfica, objetiva-se analisar o uso da IA na fiscalização tributária, com destaque à fiscalização aduaneira, e os efeitos de sua aplicação quanto aos direitos fundamentais.

1 ATIVIDADE FISCALIZATÓRIA NO ESTADO DEMOCRÁTICO DE DIREITO

A República Federativa brasileira, formada a partir da união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado Democrático de Direito[2] (art. 1º da CF/88[3]), cuja função principal é a tutela dos direitos fundamentais, bem como a consecução dos objetivos fundamentais da República dispostos no art. 3º da CF/88[4].

[2] O Estado democrático de direito, a toda evidência, é a conjugação do Estado de direito com o regime democrático. Trata-se, portanto, do Estado submetido ao império da lei, ou seja, a um conjunto de normas (constitucionais e infraconstitucionais) que criam seus órgãos e estabelecem suas competências, que preveem a separação de poderes, e que explicitam os direitos e garantias fundamentais, com estrito respeito ao princípio democrático. (DANTAS, 2024, p. 262).

[3] Art. 1º A República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado Democrático de Direito e tem como fundamentos (BRASIL, 1988).

[4] Art. 3º Constituem objetivos fundamentais da República Federativa do Brasil: I - construir uma sociedade livre, justa e solidária; II - garantir o desenvolvimento nacional; III - erradicar a pobreza e a marginalização e reduzir as desigualdades sociais e regionais; IV - promover o bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação. (BRASIL, 1988).

Para atingir as suas finalidades, o Estado Democrático de Direito tem como pilar fundamental a noção de *separação de poderes*, que os divide em três *funções* precípuas[5]: o Legislativo (criação de leis), o Judiciário (resolução de conflitos por meio da jurisdição) e o Executivo (administração dos interesses públicos).

Essa organização está intimamente ligada à Teoria dos Freios e Contrapesos de Montesquieu, a partir da qual "*é preciso que, pela disposição das coisas, o poder freie o poder*" (Montesquieu, 2005, p.118 apud AMARAL JÚNIOR, 2008, p. 02), como forma de impedir ou inviabilizar abusos. Isto é, embora sejam definidas constitucionalmente funções típicas para os três poderes, em consonância com a sua competência principal, também são designadas funções atípicas, em que um mesmo poder pode apresentar atividades legislativas, executivas e de julgamento (ZAFFARI et al., 2020), sem que isso represente invasão ilegítima nas competências constitucionalmente previstas.

É precisamente nesse ponto que emerge a necessidade de adentrar à esfera do Poder Executivo, em que a Administração Pública possui como prerrogativas constitucionais a atividade de fomento, o serviço público e a atividade de polícia administrativa. Manifestamente, as fiscalizações e sanções realizadas no âmbito tributário encontram-se nesta última atribuição, sendo imputada à Secretaria da Receita Federal do Brasil (SRFB), no âmbito da União, e às Secretarias da Fazenda no âmbito estadual, municipal e do Distrito Federal[6].

A atividade fiscalizatória da Administração pode ser entendida sob duas perspectivas: preventiva e repressiva. No caráter preventivo, os agentes visam evitar a ocorrência de danos sociais por meio da vigilância e controle de condutas. Já no caráter repressivo, quando a norma de polícia é violada, a atuação envolve a imposição de sanções, geralmente materializadas por meio de obrigações de fazer ou não fazer, com o objetivo de corrigir ou punir a transgressão, restaurando o cumprimento das normas legais. (CARVALHO FILHO, 2023, P. 75).

Cumpre mencionar, finalmente, que os atos administrativos, e consequentemente a fiscalização tributária, revestem-se de princípios próprios do Direito Público, como a presunção de legitimidade, presunção de veracidade, imperatividade, autoexecutoriedade e tipicidade.

[5] Art. 2º São Poderes da União, independentes e harmônicos entre si, o Legislativo, o Executivo e o Judiciário. (BRASIL, 1988)

[6] Art. 1º A Secretaria da Receita Federal passa a denominar-se Secretaria da Receita Federal do Brasil, órgão essencial ao funcionamento do Estado, de caráter permanente, estruturado de forma hierárquica e diretamente subordinado ao Ministro de Estado da Fazenda e que tem por finalidade a administração tributária e aduaneira da União. (BRASIL, 1988).

As presunções de legitimidade e de veracidade tratam do fato de se presumir que os atos administrativos foram realizados em observância à lei e que as alegações por eles feitas são verdadeiras; a imperatividade permite a imposição do ato a terceiros sem a sua anuência; a autoexecutoriedade estipula que os atos serão realizados sem a intervenção judicial; e a tipicidade impõe que os atos administrativos não podem ser discricionários em sua integralidade, mas devem ser embasados em disposições legais preexistentes.

1.1 Previsão Legal para Atividade Fiscalizatória

O poder fiscalizatório da Administração Pública encontra respaldo no artigo 145, §1º da Constituição Federal, que dispõe:

> Art. 145, §1º. Sempre que possível, os impostos terão caráter pessoal e serão graduados segundo a capacidade econômica do contribuinte, facultado à administração tributária, especialmente para conferir efetividade a esses objetivos, identificar, respeitados os direitos individuais e nos termos da lei, o patrimônio, os rendimentos e as atividades econômicas do contribuinte. (BRASIL, 1988).

No âmbito do Código Tributário Nacional (CTN), há previsão da atividade fiscalizatória pelas autoridades administrativas (art. 194)[7], entretanto, não há especificação dos procedimentos de fiscalização ou do processo administrativo fiscal, concedendo a regulamentação de tais mecanismos aos entes tributantes por meio de suas próprias regras e leis, desde que atendam aos direitos e garantias individuais, bem como às limitações ao poder de tributar.

Cabe ressaltar, ainda, que o CTN dispõe sobre a prestação mútua de assistência para fiscalização entre a União, Estados, Municípios e Distrito Federal (art. 199)[8]. Tal disposição atua como forma de ampliar as informações coletadas para fins de controle e investigação de condutas ilícitas, caracterizando exceção ao sigilo fiscal previsto no mesmo diploma legal.

[7] Art. 194. A legislação tributária, observado o disposto nesta Lei, regulará, em caráter geral, ou especificamente em função da natureza do tributo de que se tratar, a competência e os poderes das autoridades administrativas em matéria de fiscalização da sua aplicação.
Parágrafo único. A legislação a que se refere êste artigo aplica-se às pessoas naturais ou jurídicas, contribuintes ou não, inclusive às que gozem de imunidade tributária ou de isenção de caráter pessoal. (BRASIL, 1966).

[8] Art. 199. A Fazenda Pública da União e as dos Estados, do Distrito Federal e dos Municípios prestar-se-ão mutuamente assistência para a fiscalização dos tributos respectivos e permuta de informações, na forma estabelecida, em caráter geral ou específico, por lei ou convênio.
Parágrafo único. A Fazenda Pública da União, na forma estabelecida em tratados, acordos ou convênios, poderá permutar informações com Estados estrangeiros no interesse da arrecadação e da fiscalização de tributos. (BRASIL, 1966).

1.2 Relevância da Fiscalização Tributária

Partindo de um contexto mais amplo, nota-se que a manutenção do funcionamento da máquina estatal depende diretamente da arrecadação de tributos e de seu correto controle, garantindo recursos para implementação de políticas públicas e investimentos em serviços essenciais. Sua importância é tamanha que a Constituição, em seu art. 167, IV, estabelece uma exceção à regra da não vinculação de receitas de impostos, permitindo a destinação específica de recursos para a administração tributária, assegurando a eficiência na gestão fiscal e o cumprimento das obrigações estatais para com a sociedade.

Para além dos aspectos supramencionados, a fiscalização tributária atua no combate de uma série de condutas ilícitas, tais como:

> a) Sonegação Fiscal: A fiscalização detecta omissões ou distorções nos registros de rendimentos e patrimônio, aplicando penalidades e exigindo o pagamento correto dos tributos.
>
> b) Contrabando: Atua em parceria com outros órgãos de controle, apreendendo mercadorias importadas ilegalmente e impedindo sua circulação no mercado interno.
>
> c) Descaminho: Verifica o pagamento de tributos sobre mercadorias importadas legalmente, mas sem recolhimento adequado de impostos.
>
> d) Fraudes: Identifica manipulações contábeis e declarações falsas, corrigindo o valor dos tributos devidos e punindo os responsáveis.

Por outro lado, como bem observado por Hugo de Brito Machado, a fiscalização tributária, transformada em competência pela Constituição, deve respeitar dois limites fundamentais: a legalidade e os direitos individuais. Isso implica que as ações fiscalizatórias precisam estar amparadas em lei e, ao mesmo tempo, não podem violar as garantias individuais asseguradas pela Constituição:

> Para conferir efetividade aos princípios da pessoalidade e da capacidade contributiva, a fim de que todos paguem seus tributos em obediência aos mesmos, a Constituição facultou à Administração Tributária identificar o patrimônio, os rendimentos e as atividades econômicas do contribuinte. Legitimou, em outros termos, o poder de fiscalizar, transformando-o em competência. É importante observar, porém, dois importantes limites estabelecidos à atividade de fiscalização: a legalidade e o respeito aos direitos individuais. Assim, em suma, as atribuições fiscalizatórias devem contar com previsão e disciplinamento em lei e, além disso, essa lei, para ser válida, não pode

> desrespeitar os direitos individuais (CF/88, art. 145, § 1º). (MACHADO, 2024, p. 221).

Nesse sentido, a colaboração dos contribuintes não se resume ao pagamento de quantia, mas ao cumprimento cívico de manter o funcionamento de Estado Democrático de Direito e de todos os direitos e garantias individuais constitucionalmente assegurados. Entretanto, é necessário destacar também que, embora a atividade fiscalizatória seja de extrema importância, ela também é permeada de limitações.

2 USO DA INTELIGÊNCIA ARTIFICIAL NA FISCALIZAÇÃO ADUANEIRA

A fiscalização aduaneira, regulamentada pelo Decreto 6.759/2009 e realizada pela Receita Federal do Brasil nos recintos aduaneiros, é responsável pelo controle de pessoas, bagagens e mercadorias que cruzam as fronteiras do país. Seu objetivo é assegurar a legalidade nas operações de importação e exportação, garantir o correto recolhimento de tributos e identificar ilícitos e erros nas declarações de mercadorias.

Diante de sua extrema importância, tanto do ponto de vista econômico quanto em relação à segurança nacional, o seu procedimento fiscalizatório dispõe de análise criteriosa das mercadorias pelos Auditores-Fiscais com o objetivo de identificar irregularidades.

2.1 Fiscalização Aduaneira

O procedimento fiscalizatório, no âmbito da importação, é instaurado a partir do registro da declaração de importação (DI), momento em que a mercadoria é submetida à RFB e registrada no Sistema Integrado de Comércio Exterior (Siscomex), dando início ao despacho de importação e posterior distribuição dessas DIs para um Auditor-Fiscal (com exceção do canal verde), conforme dispõe o artigo 545 do decreto 6.759/2009: “Tem-se por iniciado o despacho de importação na data do registro da declaração de importação. [...] O registro da declaração de importação consiste em sua numeração pela Secretaria da Receita Federal do Brasil, por meio do SISCOMEX” (BRASIL, 2009).

Nesta fase, são designados canais específicos de acordo com a necessidade de apuração de possíveis irregularidades, seu grau de risco e a relevância dessas potenciais inconsistências acerca das informações apresentadas na DI. O canal verde é caracterizado pelo desembaraço automático, com posterior entrega da mercadoria, não sendo necessária a análise

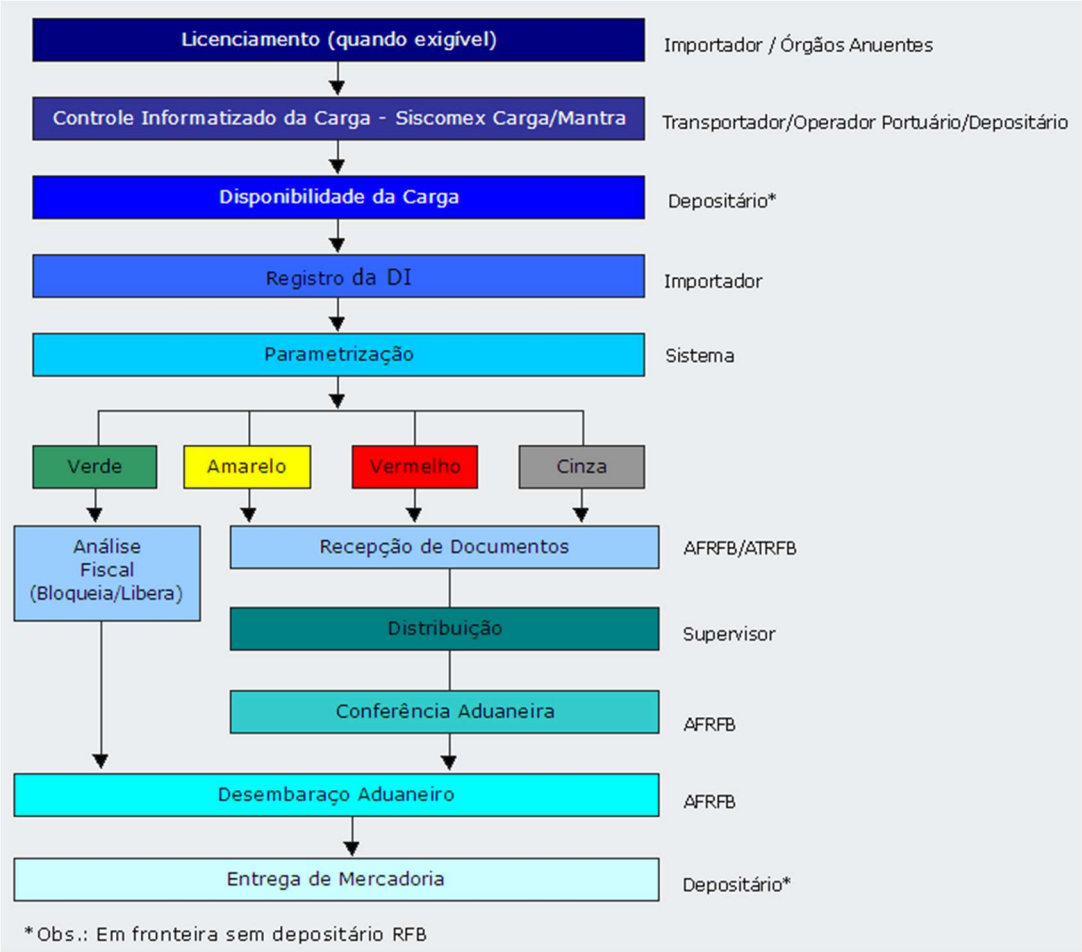
de documentações ou a verificação física do produto. Em contraste, o canal amarelo exige a realização de análise documental. O canal vermelho condiciona o desembaraço às verificações física e documental, devido ao seu maior risco de irregularidades ou erros. Por fim, o canal cinza apresenta a necessidade das duas etapas de fiscalização, além da investigação de possíveis fraudes e ilícitos. Destaca-se também que, frente a indícios de irregularidades, qualquer dos canais pode apresentar análise mais aprofundada, sendo objeto das conferências estabelecidas (BRASIL, 2006).

Assim, para os canais amarelo, vermelho e cinza, o importador deve anexar toda documentação necessária, sob pena de a mercadoria ser considerada abandonada, caso permaneça omisso durante o prazo estipulado (BRASIL, 2009). Ulteriormente, dá-se início à fase de conferência aduaneira, que consiste na análise, pelo agente da RFB, de informações como a classificação fiscal, natureza e todos outros dados e documentos previamente demandados, a fim de conferir as possíveis irregularidades e erros de forma mais aprofundada, conforme prevê a legislação brasileira[9].

Em conclusão ao procedimento de fiscalização dos produtos importados, há o desembaraço aduaneiro e a entrega da mercadoria, procedimentos condicionados a eventuais correções de irregularidades na DI, a exemplo do estabelecido na lei: “A mercadoria objeto de exigência fiscal de qualquer natureza, formulada no curso do despacho aduaneiro na forma do caput do art. 42, somente será desembaraçada após o respectivo cumprimento”. (BRASIL, 2006).

FIGURA 1 - DESPACHO DE IMPORTAÇÃO

[9] Art. 564. A conferência aduaneira na importação tem por finalidade identificar o importador, verificar a mercadoria e a correção das informações relativas a sua natureza, classificação fiscal, quantificação e valor, e confirmar o cumprimento de todas as obrigações, fiscais e outras, exigíveis em razão da importação. (BRASIL, 2009).



(BRASIL, 2020).

2.2 Sisam: A Inteligência Artificial usada pela Receita Federal do Brasil na Fiscalização Aduaneira

Levando em consideração a quantidade de procedimentos a serem realizados e diante da alta demanda quanto à quantidade de mercadorias a serem vistoriadas, nota-se que o número de Agentes Fiscais é insuficiente para a análise detalhada de cada item que possa apresentar irregularidades, ainda que em menor grau. Além disso, é necessário destacar o fato de que a escolha de tais produtos a serem vistoriados por amostragem, por esses auditores, acaba por não apresentar máxima eficiência.

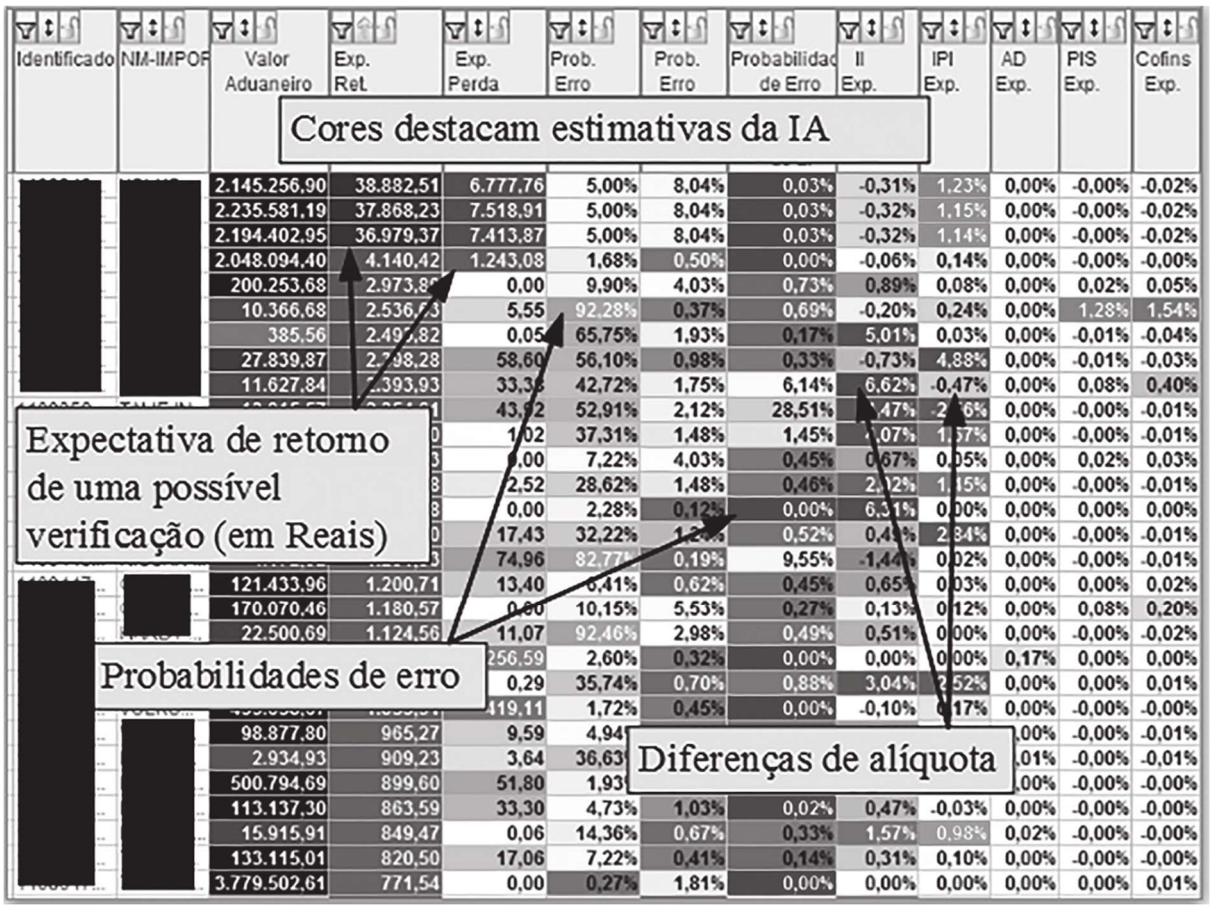
Dessa forma, como alternativa para tornar o procedimento fiscalizatório mais célere e assertivo, a RFB desenvolveu o Sistema de Seleção Aduaneira por Aprendizado de Máquina (Sisam), inteligência artificial implementada a partir de 2014, capaz de identificar quais declarações têm maior probabilidade de conter irregularidades, além de fundamentar suas

colocações em linguagem natural, auxiliando de forma direta os agentes e facilitando a correção de possíveis equívocos.

O Sisam, a partir do extenso histórico de importações do Siscomex, está apto a comparar as versões originais e desembaraçadas das DIs anteriormente verificadas, possibilitando a identificação de erros recorrentes. A IA está disponível em todas unidades voltadas à fiscalização aduaneira da Receita Federal do Brasil de forma interligada ao Siscomex e apresenta suas análises dentro do Analisador Inteligente e Integrado de Transações Aduaneiras (Aniita). (JAMBEIRO FILHO, 2015, p.16).

De forma geral, o Sistema tem sua atuação principal no encaminhamento das DIs aos canais de conferência corretos e na identificação, por meio da análise de diversos dados, de quais mercadorias devem ser priorizadas quanto à vistoria física. Seus resultados são apresentados por meio de uma planilha, que reúne dados como o valor aduaneiro, a expectativa de retorno, a probabilidade de erro e a diferença de alíquota, além da identificação da operação e do importador.

Figura 1: Planilha-padrão do Sisam

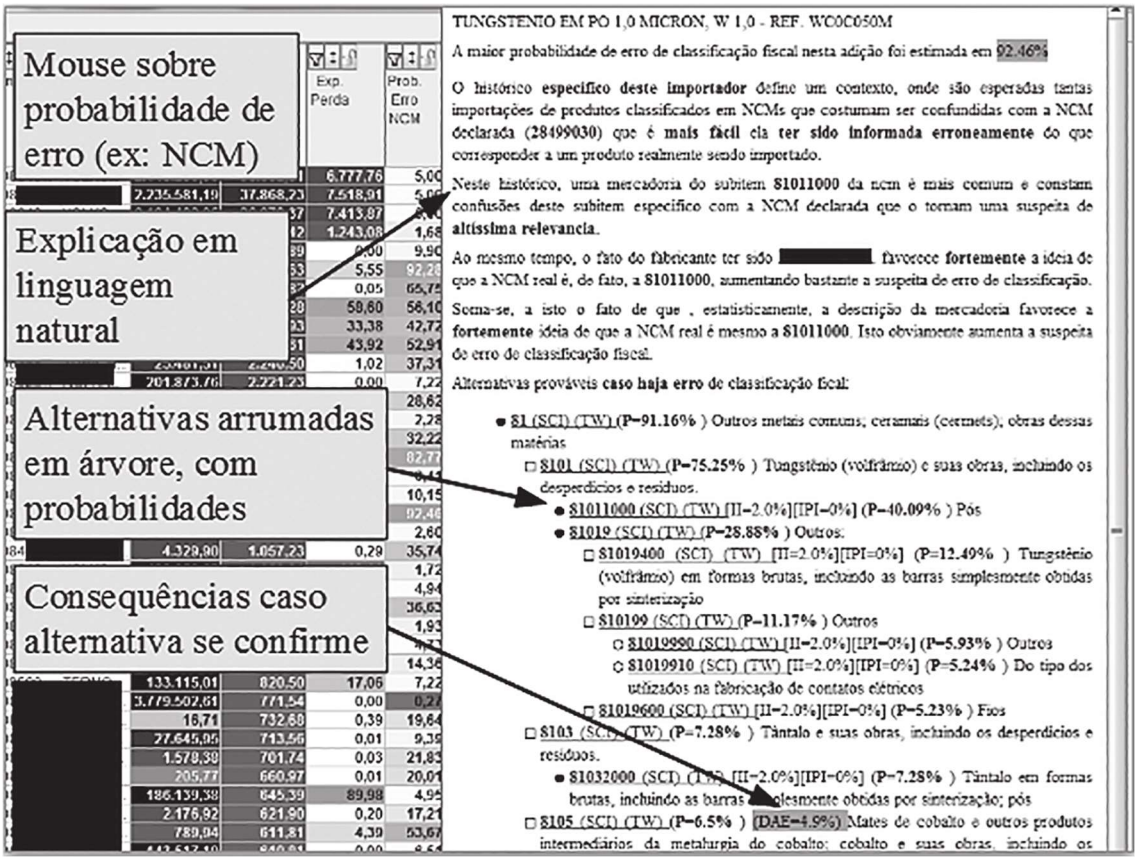


Fonte: JAMBEIRO FILHO, 2015.

O fato de o sistema apresentar, de forma concisa e padronizada, as informações a serem analisadas pelo fiscal, além de utilizar as cores para indicar maior ou menor probabilidade de erro ou de divergências em alíquotas, facilita a interação com o ser humano e torna o sistema intuitivo. Destaca-se também o campo referente à expectativa de retorno que, de acordo com Jambeiro Filho, "orienta o fiscal para que ele aproveite bem seu tempo e sua energia".

Um dos aspectos mais relevantes do Sisam é a habilidade de comunicar, em linguagem natural, o ponto exato de erro potencial, além de apresentar probabilidades realistas e conexões de ideias pertinentes quanto às inconsistências nas informações da mercadoria, podendo identificar até mesmo problemas relacionados à classificação fiscal, um dos erros mais complexos de serem solucionados. Conforme a imagem e o trecho abaixo, referente a uma análise do sistema, é possível identificar como a comunicação com o Auditor-Fiscal é realizada.

Figura 2: Justificativa de suspeita na NCM e sugestões.



Fonte: JAMBEIRO FILHO, 2015. [10]

O Sisam, aliado à inteligência natural dos Auditores-Fiscais, teve como resultado a detecção de erros em mais de 75% das declarações selecionadas, a partir da sugestão do sistema, para inspeção física.

Entretanto, embora o uso da IA promova melhora significativa no processo fiscalizatório aduaneiro, surgiram preocupações quanto à ética de sua aplicação devido ao desconhecimento sobre a forma como o sistema chega às suas conclusões. Como forma de solucionar tal problema, o Sisam gera explicações e tem a habilidade de demonstrar sua linha de raciocínio, tornando-se inteiramente auditável. (JAMBEIRO FILHO, 2020).

3 O USO DA IA FRENTE AOS DIREITOS FUNDAMENTAIS DO CONTRIBUINTE E ASPECTOS ÉTICOS E JURÍDICOS

Diante do ineditismo do emprego da Inteligência Artificial no âmbito da Administração Pública em proporções tão abrangentes, há que se debruçar, para além de seus impactos positivos quanto à produtividade e eficiência, sobre seus efeitos nos direitos fundamentais do contribuinte e nos aspectos jurídicos e éticos relacionados ao seu funcionamento.

3.1 Critérios de Seleção

O direcionamento do Auditor-Fiscal pelo Sisam, quanto às mercadorias a serem vistoriadas, apresenta critério de seleção baseado, predominantemente, em dados probabilísticos de cunho econômico. Tal visão é evidenciada por colocação de Jambeiro Filho acerca da coluna da planilha referente à expectativa de retorno:

[10] Transcrição do texto gerado automaticamente pelo Sisam ao analisar caso real: "A probabilidade de erro de classificação fiscal neste item foi estimada em 92.46%. O histórico específico deste importador define um contexto, onde são esperadas tantas importações de produtos classificados em NCMs que costumam ser confundidas com a NCM declarada (28499030) que é mais fácil ela ter sido informada erroneamente do que corresponder a um produto realmente sendo importado. Neste histórico, uma mercadoria do subitem 81011000 da NCM é mais comum e constam confusões deste subitem específico com a NCM declarada que o tornam uma suspeita de altíssima relevância. Ao mesmo tempo, o fato do fabricante ter sido XXXXXX S.A. favorece fortemente a ideia de que a NCM real é, de fato, a 81011000, aumentando bastante a suspeita de erro de classificação. Soma-se, a isto o fato de que, estatisticamente, a descrição da mercadoria favorece a fortemente ideia de que a NCM real é mesmo a 81011000. Isto obviamente aumenta a suspeita de erro de classificação fiscal." (JAMBEIRO FILHO, 2015).

> A expectativa de retorno orienta o fiscal para que ele aproveite bem seu tempo e sua energia. Uma mercadoria de valor médio pode ter uma expectativa de retorno alta se as probabilidades de erro forem altas. Uma mercadoria de pouco valor pode ter a expectativa de retorno alto se houver probabilidades de erro altas com consequências administrativas importantes, como uma fuga de licença de importação. Já uma mercadoria de muito valor pode merecer a atenção do fiscal ainda que as probabilidades de erro sejam relativamente baixas. (JAMBEIRO FILHO, 2015, p. 28).

Embora o uso dessas informações como forma de guiar a fiscalização tributária pareça óbvio, há de se considerar que o emprego do método quantitativo pela IA pode desconsiderar dados de cunho jurídico importantes para o Estado Democrático de Direito, favorecendo a vistoria física de mercadorias que tenham o condão de apresentar impacto financeiro favorável ao maior recolhimento do Estado em detrimento daquelas que, mesmo irregulares, não apresentam expectativa de retorno alta.

O sistema dispõe, em sua planilha, de uma coluna denominada expectativa de perda, em que é calculada a probabilidade de a mercadoria apresentar erros que resultem em valores em benefício do contribuinte. Nesses casos o auditor, dentro de sua discricionariedade, pode decidir se irá destinar sua atenção a corrigir a diferença ou não. Entretanto, é de se questionar se o sistema, por se pautar em critérios econômicos, não facilita e preconiza o tipo de exame que favoreça a análise em favor do recolhimento da RFB, e não a fiscalização baseada em preceitos éticos.

> A luz dos parâmetros constitucionais, a (in)adequação jurídica da ação do contribuinte deveria ser objeto de controle estatal independente da consequência financeira que gerasse aos cofres públicos. Em outras palavras, em termos jurídicos, a fiscalidade deveria ser orientada pela conformidade legal. Esse é o significado de um Estado de Direito. Portanto, devemos entender como prejuízo toda a ação do Estado ou do contribuinte que não esteja em conformidade com a lei, independente do seu resultado financeiro. Quando se trata de fiscalidade, um prejuízo jurídico será sempre maior que um prejuízo financeiro, pois sua base será sempre uma violação ao princípio democrático. (KÖCHE, 2020, p. 194).

Nesse sentido, para que o método utilizado pela Inteligência Artificial em questão seja considerado legítimo quanto aos aspectos jurídicos, deve-se partir de uma visão teórica utilitarista, num contexto em que o utilitarismo estaria ligado ao consequencialismo. (KÖCHE, 2020). Tal corrente ética utiliza as consequências como forma de avaliar as ações, medindo assim, a sua utilidade, como define Bentham: “Por princípio de utilidade entende-se aquele princípio que aprova ou desaprova qualquer ação, segundo a tendência que tem a aumentar ou a diminuir a felicidade da pessoa cujo interesse está em jogo [...]”. (BENTHAM, 1974, p.10).

Dessa forma, o ato de estabelecer o que é uma prioridade na fiscalização, no Estado Democrático de Direito, partindo de uma escolha entre o mais viável e proveitoso economicamente e o mais legítimo de acordo com o princípio democrático, evidentemente traz diversos pontos que chamam atenção para o uso da Inteligência Artificial.

3.2 Lei Geral de Proteção de Dados

Frente ao extenso banco de dados utilizado pelo Sisam, composto pelo histórico de Declarações de Importação registradas no Siscomex desde 1997, e ao advento da Lei Geral de Proteção de Dados (LGPD), que dispõe sobre o tratamento de dados pessoais objetivando a proteção da liberdade e privacidade, surge a preocupação acerca do uso de dados pela IA e suas consequências.

Um dos aspectos mais significativos da lei supracitada, é a preocupação com a adoção de medidas de segurança eficazes que tenham por finalidade a proteção das informações do indivíduo[11] (art. 46 da lei 13.709/2018). Destaca-se que tal medida visa dirimir a possibilidade do uso de dados pessoais de forma indiscriminada, seja por meio de vazamento de dados ou erro interno, acarretando a violação ao princípio da privacidade.

Nesse sentido, cabe ao órgão fiscalizador o tratamento de dados de forma responsável e ponderada, sendo facultada a implementação de mecanismos voltados à garantia da proteção de informações sensíveis do contribuinte, que podem dispor de regras de boas práticas e de segurança[12] (art. 50 da lei 13.709/2018). Além disso, a IA deve ser manipulada corretamente por todos usuários e agentes responsáveis pelo sistema, a fim de não representar um obstáculo à preservação da privacidade e segurança do contribuinte.

[11] Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.
§ 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei. (BRASIL, 2018).

[12] Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais. (BRASIL, 2018).

Dentro desse contexto, considerando que o Sisam dispõe de banco de dados extremamente extenso, composto pelas Declarações de Importação e também pelos resultados das análises realizadas, é de extrema importância o correto manuseio desses dados e a implementação de procedimentos que visem minimizar quaisquer riscos à segurança das informações armazenadas. Além disso, considerando que a IA tem sua atuação interligada a sistemas como o Siscomex e o Aniita, é essencial que todos esses programas trabalhem essa questão de forma concomitante, evitando prejuízos ao tributário.

O diploma legal prevê, também, a necessidade de transparência no tratamento de dados[13] (art. 9º da lei 13.709/2018), um desafio na aplicação da Inteligência Artificial em vista do desconhecimento, pelo agente que acessa a informação disponibilizada, de todo processo realizado pela máquina para chegar a determinada conclusão. Nesse ponto, devido à linguagem natural, o Sisam se destaca por ter a habilidade de demonstrar com clareza quais foram os dados utilizados e quais conexões foram feitas para a identificação do erro, aumentando significativamente a transparência em todo processo, além de tornar o sistema inteiramente auditável.

Além disso, um ponto relevante quanto ao princípio da transparência é o considerável desconhecimento, pelo próprio contribuinte, do uso da Inteligência Artificial e dos mecanismos utilizados por ela na fiscalização aduaneira. Embora se trate de um procedimento interno, próprio do procedimento fiscalizatório, o tributário deve tomar conhecimento de novas ferramentas utilizadas pela Administração para tal finalidade, garantindo a percepção de legalidade do controle fiscal.

Ademais, é de suma importância que o auto de infração[14] (art. 10 do decreto 70.235/1972), por meio do qual o contribuinte é alertado sobre ilegalidades e irregularidades da mercadoria, esteja munido de informações claras e precisas, que auxiliem o destinatário a

[13] Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso: I - finalidade específica do tratamento; II - forma e duração do tratamento, observados os segredos comercial e industrial; III - identificação do controlador; IV - informações de contato do controlador; V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade; VI - responsabilidades dos agentes que realizarão o tratamento; e VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei. (BRASIL, 2018).

[14] Art. 10. O auto de infração será lavrado por servidor competente, no local da verificação da falta, e conterá obrigatoriamente: I - a qualificação do autuado; II - o local, a data e a hora da lavratura; III - a descrição do fato; IV - a disposição legal infringida e a penalidade aplicável; V - a determinação da exigência e a intimação para cumpri-la ou impugná-la no prazo de trinta dias; VI - a assinatura do autuante e a indicação de seu cargo ou função e o número de matrícula. (BRASIL, 1972).

identificar precisamente o erro e a evitar que ele se repita. Assim, a aplicação da ferramenta deve facilitar a lavratura do auto de infração permitindo que o Auditor-Fiscal descreva, com agilidade, os erros encontrados com riqueza de detalhes.

Em síntese, é necessário que a fiscalização não desrespeite a proteção de dados legalmente prevista ou os princípios da privacidade e transparência. Embora o controle fiscal seja crucial para a manutenção do funcionamento do Estado, o anseio pelo melhoramento dos sistemas de IA, como forma de atingir essa finalidade, não deve colocar em risco os direitos e garantias preconizados na legislação brasileira.

CONCLUSÃO

Diante da relevância da atividade fiscalizatória para a manutenção do funcionamento do Estado Democrático de Direito, nota-se que o uso da Inteligência Artificial, de forma abrangente e significativa, propiciou o aprimoramento de procedimentos complexos e demorados, além de impactar positivamente os resultados, tornando-os mais assertivos.

No âmbito aduaneiro, a implementação do Sisam foi extremamente bem-sucedida, servindo como ponto de partida para o desenvolvimento de diversas outras tecnologias voltadas à atividade de polícia administrativa, realizada pela Administração. Destaca-se também que, embora a IA atue na parametrização de mercadorias, direcionando o Auditor-Fiscal em relação às que devem dispor de vistoria física, ela representa apenas um auxílio, permitindo que a tomada de decisão seja realizada diretamente pelo profissional.

Em complemento, a capacidade de comunicar, em linguagem natural, quais foram as irregularidades encontradas e quais informações utilizadas para chegar a determinada conclusão, permite maior transparência no procedimento fiscalizatório e facilita a identificação e a correção de eventuais erros do sistema de forma célere e eficaz.

Em que pese os direitos fundamentais, a aplicação de sistemas de IA ainda representa um ponto de atenção frente aos princípios da privacidade e da transparência, principalmente quanto à segurança das informações e à possibilidade de uso indevido de dados pessoais do contribuinte. Evidentemente, tal problemática não é exclusiva ao uso da tecnologia em questão no processo fiscalizatório, mas uma característica comum a sistemas que utilizam bancos de dados.

Assim, é notável a importância do uso desses sistemas para fins de aprimoramento da fiscalização tributária, em vista de seu excelente desempenho quanto à capacidade de análise e de confronto de informações. Contudo, ressalta-se a necessidade de observar constantemente se o uso da tecnologia está em consonância com a legislação e se a sua aplicação não implica em violação aos direitos fundamentais do contribuinte.

REFERÊNCIAS

AMARAL JÚNIOR, José Levi Mello do. Sobre a organização de poderes em Montesquieu: comentários ao Capítulo VI do Livro XI de O Espírito das Leis. **Revista dos Tribunais**, São Paulo, v. 868, 2008. Disponível em: https://edisciplinas.usp.br/pluginfile.php/5572274/mod_resource/content/0/Organizacao%20de%20poderes%20em%20Montesquieu.pdf. Acesso em: 03 out. 2024.

BENTHAM, Jeremy. Uma Introdução aos princípios da moral e da legislação. 1. ed. São Paulo: **Abril Cultural**, 1974. Disponível em: https://edisciplinas.usp.br/pluginfile.php/7576356/mod_resource/content/1/10.%20BENTHAM%3B%20MILL.pdf. Acesso em: 15 out. 2024.

BESSA, Leonardo Roscoe. LGPD – proteção à privacidade ou aos dados pessoais?. **Tribunal de Justiça do Distrito Federal e dos Territórios – TJDFT**, Brasília/DF, 2024. Disponível em: https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/artigos-discursos-e-entrevistas/artigos/artigo-lgpd-2013-protecao-a-privacidade-ou-aos-dados-pessoais. Acesso em: 03 out. 2024.

BRASIL. **Receita Federal.** Despacho de importação - DI. Publicado em 2014. Atualizado em 2020. Disponível em: https://www.gov.br/receitafederal/pt-br/assuntos/aduana-e-comercio-exterior/manuais/despacho-de-importacao/topicos-1/despacho-de-importacao/etapas-do-despacho-aduaneiro-de-importacao/despacho-de-importacao-di. Acesso em: 15 out. 2024.

BRASIL. **Receita Federal.** Etapas do despacho aduaneiro de importação. Publicado em 2014. Atualizado em 2022. Disponível em: https://www.gov.br/receitafederal/pt-br/assuntos/aduana-e-comercio-exterior/manuais/despacho-de-importacao/topicos-1/despacho-de-importacao/etapas-do-despacho-aduaneiro-de-importacao. Acesso em: 12 out. 2024.

CARVALHO FILHO, José dos Santos. **Manual de Direito Administrativo**. 37. ed. Rio de Janeiro: Atlas, 2023. E-book. ISBN 9786559774265. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9786559774265/. Acesso em: 15 out. 2024.

DANTAS, Paulo Roberto de Figueiredo. **Curso de direito constitucional**. 7. ed. Indaiatuba, SP: Foco, 2024. E-book. Disponível em: https://plataforma.bvirtual.com.br.

JAMBEIRO FILHO, Jorge Eduardo de Schoucair. Artificial Intelligence in the Customs Selection System through Machine Learning (SISAM). **Prêmio de Criatividade e Inovação da RFB.** Brasília: Receita Federal do Brasil, 2015.

JAMBEIRO FILHO, Jorge Eduardo de Schoucair. Brazil: Artificial intelligence in Brazil's Customs. **WCO/WTO Study Report on Disruptive Technologies**: Bruxelas, 2022.

KÖCHE, Rafael. Inteligência artificial a serviço da fiscalidade: sistema de seleção aduaneira por aprendizado de máquina (SISAM). In: MACHADO, Hugo de Brito (Coord.). **Tributação e novas tecnologias**. São Paulo: Editora Foco, 2021. Disponível em: https://www.rafaelkoche.com.br/arquivos/TRIBUTACAO-E-NOVAS-TECNOLOGIAS-Rafael-Koche.pdf. Acesso em: 12 out. 2024.

MACHADO SEGUNDO, Hugo de Brito. **Manual de Direito Tributário**. 14. ed. Rio de Janeiro: Atlas, 2024. E-book. ISBN 9786559776177. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9786559776177/. Acesso em: 15 out. 2024.

PISKE, Oriana; SARACHO, Antonio Benites. Considerações sobre a teoria dos freios e contrapesos (checks and balances system). **Tribunal de Justiça do Distrito Federal e dos Territórios – TJDFT**, 2018. Disponível em: https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/artigos-discursos-e-entrevistas/artigos/2018/consideracoes-sobre-a-teoria-dos-freios-e-contrapesos-checks-and-balances-system-juiza-oriana-piske. Acesso em: 10 out. 2024.

JANINI, Tiago Cappi; PULCINELLI, Ana Luiza Godoy. A fiscalização tributária e seus limites: uma análise a partir do princípio da legalidade e dos direitos fundamentais do contribuinte. **Revista de Direito Tributário e Financeiro**, Curitiba, v. 2, n. 2, p. 347-365, jul./dez. 2016. e-ISSN: 2526-0138.

ZAFFARI, Eduardo K.; SILVA, Maira J F.; MIÃO, João R.; et al. **Fiscalização tributária**. Porto Alegre: SAGAH, 2020. E-book. p.19. ISBN 9788533500679. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9788533500679/. Acesso em: 11 out. 2024.

7 Information Society and Law
FMU CENTRO UNIVERSITÁRIO

DIGITALIZAÇÃO E TEORIA DA PROVA: UMA ANÁLISE CONTEMPORÂNEA

DIGITALIZATION AND THEORY OF EVIDENCE: A CONTEMPORARY ANALYSIS

Edielma Rocha Dutra[1]; Tiago Cappi Janini[2]

Resumo: A sociedade da informação trouxe mudanças significativas em diversos campos do conhecimento, incluindo o direito. Este artigo investiga o impacto da digitalização sobre a teoria da prova, considerando as profundas transformações ocasionadas pela sociedade da informação. O problema de pesquisa gira em torno de como a digitalização, combinada com a ampla disponibilidade de dados digitais, altera os fundamentos tradicionais da prova jurídica, especialmente no que se refere à autenticidade, integridade e preservação das evidências, com destaque para a relevância da cadeia de custódia. O objetivo principal é identificar e analisar as novas dinâmicas impostas à prática jurídica, ressaltando os desafios e oportunidades que emergem na coleta, preservação e apresentação de provas digitais. A metodologia empregada consiste na análise de bibliografia especializada, incluindo doutrinas, artigos acadêmicos, teses de mestrado e doutorado, legislações aplicáveis e a jurisprudência sobre o tema. Além disso, foram consideradas discussões contemporâneas acerca da privacidade e da segurança no manejo de dados digitais. Conclui-se que, no contexto jurídico atual, a digitalização impõe a necessidade de novas abordagens teóricas e práticas, de modo a garantir tanto a efetividade quanto a segurança jurídica na utilização das provas digitais, reafirmando a importância de uma robusta cadeia de custódia.
Palavras-chave: Sociedade da Informação; ecossistema digital; segurança dos dados pessoais; teoria da prova; provas digitais.

Abstract: The information society has brought significant changes across various fields of knowledge, including law. This article investigates the impact of digitalization on proof theory, considering the profound transformations caused by the information society. The research problem revolves around how digitalization, combined with the wide availability of digital data, changes the traditional foundations of legal evidence, especially with regard to authenticity, integrity and preservation of evidence, with emphasis on the relevance of the chain of custody. The main objective is to identify and analyze the new dynamics imposed on legal practice, highlighting the challenges and opportunities that emerge in the collection, preservation and presentation of digital evidence. The methodology used consists of the analysis of specialized

[1] Oficial de Promotoria no Ministério Público do Estado de São Paulo (MPSP). Graduada pela Universidade Católica de Santos (UNISANTOS). Pós-graduada em Direito Processual Penal pela Instituto Damásio de Direito/IBMEC. Pós-graduanda em Direito Penal e Criminologia na PUC - Rio Grande do Sul. Mestranda em Direito da Sociedade da Informação nas Faculdades Metropolitanas Unidas.
[2] Doutor em Direito pela Pontifícia Universidade Católica de São Paulo. Professor do Programa de Mestrado em Direito na Sociedade da Informação e da graduação da FMU. Estágio de Pós-Doutorado na Universidade Estadual do Norte do Paraná (UENP), bolsista PNPD-CAPES.

bibliography, including doctrines, academic articles, master's and doctoral theses, applicable legislation and jurisprudence on the subject. Furthermore, contemporary discussions about privacy and security in the handling of digital data were considered. It is concluded that, in the current legal context, digitalization imposes the need for new theoretical and practical approaches, in order to guarantee both effectiveness and legal security in the use of digital evidence, reaffirming the importance of a robust chain of custody.
Keywords: Information Society; digital ecosystem; personal data security; theory of evidence; digital evidence.

INTRODUÇÃO

A Era Digital, impulsionada pela difusão de algoritmos e pela crescente digitalização das atividades humanas, trouxe mudanças substanciais para diversos campos do saber, incluindo o Direito. As interações sociais, o trabalho e as formas de comunicação foram profundamente modificados, exigindo uma reavaliação dos alicerces sobre os quais se constrói o sistema jurídico. Nesse cenário, a Teoria do Direito precisa se adaptar às novas dinâmicas, e, em especial, a Teoria da Prova, essencial no direito processual para a busca da verdade, é diretamente impactada pelas inovações tecnológicas e pela proliferação de dados digitais.

O problema de pesquisa aqui abordado é como a digitalização e a sociedade da informação afetam os conceitos tradicionais da Teoria da Prova, com ênfase na autenticidade, integridade e cadeia de custódia das provas digitais. As rápidas transformações tecnológicas exigem uma releitura dos mecanismos tradicionais de produção e valoração de provas, questionando-se até que ponto os paradigmas processuais vigentes são capazes de responder adequadamente a essas mudanças.

O objetivo deste artigo é analisar os desafios e oportunidades trazidos pela digitalização no campo da prova processual. Questões como a volatilidade dos dados digitais, a integridade e autenticidade das provas, e a adaptação das normas processuais ao ambiente digital serão discutidas à luz de doutrinas e jurisprudências. Além disso, o artigo também explora as potencialidades das tecnologias emergentes, como a inteligência artificial, na coleta e análise de evidências, buscando formas mais eficientes e seguras de garantir a verdade processual.

A metodologia aplicada é a análise crítica de bibliografia especializada, englobando estudos acadêmicos, doutrinas, legislações e jurisprudências, de forma a oferecer uma visão ampla sobre as mudanças na Teoria da Prova na era digital. Em suma, o artigo busca fomentar a reflexão sobre o futuro da Teoria da Prova em um mundo cada vez mais digital, incentivando

o debate sobre como o sistema jurídico pode se adaptar a essa nova realidade de forma justa e eficaz.

1. A SOCIEDADE DA INFORMAÇÃO E O DIREITO

A sociedade da informação é marcada pela predominância das tecnologias de informação e comunicação (TICs) e pela digitalização dos dados. Segundo Manuel Castells (1999, p. 119), essa sociedade é caracterizada pela capacidade de gerar, processar e transmitir informações de maneira eficiente. No contexto jurídico, isso significa que as provas digitais, como e-mails, mensagens de texto e registros de redes sociais, tornaram-se cada vez mais comuns.

A sociedade da informação representa uma transformação profunda na maneira como a informação é gerada, processada e disseminada. Este conceito, amplamente discutido por estudiosos como Manuel Castells, refere-se a uma era em que as tecnologias de informação e comunicação (TICs) desempenham um papel central na estruturação das sociedades modernas. A digitalização e a conectividade global são características marcantes dessa sociedade, influenciando diversos aspectos da vida cotidiana, incluindo o campo jurídico.

A sociedade da informação é definida por várias características distintivas. Dário José Kist (2024, p. 29) assim a descreve:

> a sociedade da informação e da comunicação é um “mundo” com intenso fluxo de informações, que está em veloz e permanente mudança e em que o conhecimento é flexível, fluido e sempre em expansão; as noções existentes sobre território foram relativizadas, pois superadas as barreiras que o espaço, assim como o tempo, impunham à comunicação entre as pessoas, notadamente as ausentes.

Nesse contexto, tem-se a digitalização (a conversão de informações analógicas em formato digital permite um armazenamento, processamento e transmissão mais eficientes. Isso inclui desde documentos e registros até comunicações pessoais e transações financeiras), conectividade global (a internet e outras redes de comunicação conectam indivíduos e organizações em escala global, permitindo a troca instantânea de informações), abundância de dados (a produção e o armazenamento de grandes volumes de dados, muitas vezes referidos como "big data", criam novas possibilidades para análise e tomada de decisão), velocidade de informação (a rapidez com que a informação pode ser transmitida e acessada transforma a maneira como as decisões são tomadas e como as interações sociais e comerciais ocorrem).

A introdução dessas características no contexto jurídico traz uma série de implicações. A digitalização resulta em novas formas de provas digitais, evidências digitais, como e-mails, mensagens de texto, registros de redes sociais e dados de localização. Esses tipos de provas requerem novas abordagens para autenticação e verificação. A facilidade com que dados digitais podem ser manipulados levanta questões sobre a autenticidade e a integridade das provas. Ferramentas tecnológicas e protocolos de segurança são necessários para garantir que as provas digitais sejam confiáveis.

Ademais, a conectividade global e a abundância de dados oferecem aos advogados e juízes acesso a uma quantidade sem precedentes de informações, potencialmente enriquecendo a análise de casos e a tomada de decisões. A coleta e o uso de dados digitais levantam preocupações sobre privacidade e segurança, exigindo um equilíbrio entre o uso de informações para fins legais e a proteção dos direitos individuais.

A sociedade da informação, portanto, não apenas redefine a maneira como a informação é tratada, mas também desafia e enriquece o campo jurídico, exigindo uma adaptação contínua para lidar com as novas realidades tecnológicas.

A crescente adoção de recursos digitais e o consequente armazenamento massivo de informações através do tráfego contínuo na web, impulsionado por tecnologias que são constantemente desenvolvidas, resulta no registro de grande parte das atividades diárias da sociedade. Nesse cenário, as provas digitais ganham destaque, pois essa realidade demanda um sistema que ofereça aos cidadãos todos os meios legítimos para satisfação pessoal e corporativa, utilizando tecnologias, mas sempre com atenção à segurança da informação. É importante destacar que, até pouco tempo atrás, as provas em processos judiciais eram majoritariamente físicas, com raras exceções de provas em formatos como áudio em CD ou disquete. Atualmente, no entanto, as provas digitais dominam as investigações criminais e são fundamentais na produção de evidências em processos jurídicos, que também se tornaram majoritariamente eletrônicos. As provas digitais que sustentam processos judiciais ou investigações criminais incluem desde documentos digitais, como contratos virtuais e capturas de tela de conversas em aplicativos, até vídeos e áudios anexados por meio de mídias digitais. A computação forense, por sua vez, é o ramo da criminalística focado na análise de vestígios cibernéticos, ou seja, informações armazenadas ou transmitidas digitalmente, abrangendo todos os elementos relacionados a elas.

2. A TEORIA DA PROVA NA ERA DIGITAL

A era digital trouxe uma revolução na forma como as provas são coletadas, apresentadas e analisadas nos processos judiciais. A teoria da prova, que tradicionalmente se baseava em evidências físicas e testemunhais, agora deve se adaptar a um ambiente onde as provas digitais desempenham um papel cada vez mais central.

Fazendo uma análise histórica deste fenômeno contemporâneo, Tiago Cappi Janini (2010, p. 35-36) aduz que a cibernética provocou uma verdadeira revolução, dada a evolução da internet e dos meios de transmissão de informação. Surge um ambiente onde pessoas de todos os países, pertencentes às mais diversas culturas e linguagens, encontram-se trocando informações processadas digitalmente em uma rede de computadores interconectada. Essas informações não possuem uma forma material estável no tempo e no espaço, e transcendem qualquer tipo de fronteira. Assim, emerge um novo meio social: a internet (JANINI, 2010, p. 35).

2.1. Conceitualização de "prova"

No âmbito jurídico, a prova é um elemento fundamental para a resolução de conflitos e a tomada de decisões judiciais. Em linhas gerais, a prova consiste em qualquer meio ou recurso utilizado para demonstrar a veracidade de fatos alegados pelas partes em um processo. O objetivo da prova é servir de suporte fático com o fim de convencer o juiz ou tribunal sobre a ocorrência ou não de determinados eventos, influenciando diretamente o resultado do julgamento.

Este entendimento vai ao encontro da doutrina de Cássio Scarpinella Bueno (2010, p. 261), que explica que a prova seria "tudo que puder influenciar, de alguma maneira, na formação da convicção do magistrado para decidir de uma forma ou de outra, acolhendo no todo ou em parte, ou rejeitando o pedido do autor". Da mesma forma, Luiz Guilherme Marinoni e Daniel Mitidiero (2011, p. 334) definem a prova como "meio retórico, regulado pela legislação, destinado a convencer o Estado da validade de proposições controversas no processo, dentro de parâmetros fixados pelo direito e de critérios racionais".

Tiago Cappi Janini (2010, p. 36), explicando o termo "prova" num contexto prático, aduz que:

> A "prova" como enunciação consiste nos atos produzidos para construir o fato alegado, ou seja, como ação de provar. Tomada como enunciado, "prova" seria o resultado da atividade realizada. É importante ressaltar que o vocábulo ainda é comumente usado no sentido no suporte físico. Exemplificando, usa-se a *prova* testemunhal. O processo de elaboração de uma prova testemunhal. O processo de elaboração de uma *prova testemunhal* consiste inicialmente na oitiva da testemunha, que somente ingressará nos autos quando levada a termo. Esse ato de oitiva é a *prova* na sua acepção de enunciação, como procedimento utilizado para a elaboração de um enunciado. Esse enunciado será a prova testemunhal, que consiste nas informações prestadas pela testemunha em relação ao fato alegado. Salienta-se que o enunciado está vertido em documento (suporte físico), também chamado de prova. Percebe-se, portanto, que o problema surge porque todas as etapas têm a mesma denominação: *prova*.

Modernamente, o conceito de prova ganhou novas conotações. O avanço da tecnologia trouxe novos suportes para o documento denominado prova. Tais suportes são comumente denominados de provas digitais. Trata-se de um leque amplo, que inclui e-mails, mensagens de texto, registros de chamadas telefônicas, dentre outros.

Nesse contexto, Lucien (2023, p. 39-40) define a prova digital do seguinte modo:

> Prova digital não é nada mais nada menos que todo e qualquer dado que esteja armazenado ou que seja transmitido via computador e sirva para apoiar ou para rejeitar alguma teoria sobre como um crime específico aconteceu e que contenha elementos críticos desse crime, como intenção ou álibi.

De forma mais detalhada, Alexandre Morais da Rosa (2022, n.p):

> Prova Digital (*e-evidence*). A prova digital (espécie da prova eletrônica) é a obtida e/ou produzida em ambiente eletrônico digital, em que os dados (de base, de tráfego e de conteúdo), em geral, vulneráveis, intangíveis e frágeis, devem ser extraídos e tratados em observância às normas técnicas, observada a cadeia de custódia digital, sob pena de ineficácia probatória. A tendência contemporânea é a do uso futuro da tecnologia blockchain. Definição de "e-evidence". A definição de "e-evidence" orienta-se pela: (a) relevância (meio de prova adequado ao fim que se destina); (b) confiabilidade (equivalência entre o verificado e o representado); e, (c) suficiência (deve congregar os elementos necessários de superação aos testes de verificação).

Como se vê, o conceito de prova jurídica é dinâmico e adaptável às mudanças sociais e tecnológicas, sempre buscando garantir um julgamento justo e equitativo.

Com isso, percebe-se que a prova, antes advinda de um movimento centrípeto, seja materializada num documento físico (ex.: oitiva reduzida a termo) seja materializada num documento digital (ex.: CD-ROM, pen-drive); hoje se encontra em movimento inverso, ou seja, centrífugo, cuja produção se inicia no ecossistema digital (redes sociais – Facebook, Tic Toc, Youtube, X etc.; jornais digitais; etc.). Dessa forma, importante analisar o conceito de documento eletrônico (ou digital).

2.2. Conceitualização de documento eletrônico (ou digital)

Para Rennan Thamay e Maurício Tamer (2022, n.p.), a prova, de modo geral, é o instrumento que forma a convicção de alguém em relação a um fato específico. No ecossistema digital (dispositivos, dados, usuários, plataformas, serviços online), explicam que a expressão "prova digital" pode ser interpretada de duas maneiras. A primeira interpretação considera a prova digital como a evidência de um evento que ocorreu em ambientes digitais, ou seja, um fato que depende do uso de um meio digital. A segunda interpretação sugere que, mesmo que o evento não tenha acontecido em um ambiente digital, sua comprovação pode ser feita através de meios digitais.

Os fatos ocorridos em meios digitais, para os quais a prova é necessária (prova digital), incluem situações como o envio de e-mails, mensagens por aplicativos como WhatsApp e Telegram, cópia ou desvio de bases de dados, cópia de *software*, e a publicação de vídeos na internet, sejam eles de conteúdo íntimo ou difamatório, entre outros. Além disso, o meio digital pode ser utilizado como ferramenta para comprovar a existência de um fato ocorrido fora do ambiente digital. Um exemplo seria uma ata notarial feita a partir da observação de uma foto em uma rede social, onde um funcionário de uma empresa aparece junto com um diretor de uma concorrente, demonstrando um possível conluio entre eles. No contexto criminal, o monitoramento judicialmente autorizado de conversas no WhatsApp pode fornecer provas de crimes como tráfico de drogas. Nesses casos, os fatos não são digitais por natureza, mas os meios digitais servem como um mecanismo de comprovação (THAMAY; TAMER; 2022, n.p.).

Nesse contexto, Rennan Thamay e Maurício Tamer (2022, n.p.) conceituam prova digital da seguinte forma:

> o instrumento jurídico vocacionado a demonstrar a ocorrência ou não de determinado fato e suas circunstâncias, tendo ele ocorrido total ou parcialmente em meios digitais ou, se fora deles, esses sirvam como instrumento para sua demonstração. A prova digital é o meio de demonstrar a ocorrência de um fato ocorrido em meio digital, ou que tem no meio digital um instrumento de demonstração de determinado fato de seu conteúdo.

Assim, documento eletrônico (ou digital) caracteriza-se por ser produzido, autenticado, armazenado e transmitido em formato eletrônico, mantendo sua forma original. Diversos exemplos ilustram essa categoria, como: (i) arquivos em formato PDF ou DOC, com ou sem assinatura eletrônica; (ii) vídeos criados integralmente em ambiente digital ou disponibilizados em plataformas online, como o YouTube, acessíveis por meio de QR Code; (iii) mensagens trocadas em aplicativos de mensageria instantânea, a exemplo de WhatsApp e

Telegram; (iv) e-mails; (v) arquivos de áudio em MP3 ou outros formatos, gravados inclusive em dispositivos móveis, entre outros (THAMAY; TAMER; 2022, n.p.).

Nesse contexto, alertam Rennan Tamay e Maurício Tamer (2022, n.p) que é fundamental distinguir o documento digital do digitalizado. Este último, representando um terceiro tipo documental, consiste na versão digital de um documento originalmente físico. A conversão para o meio eletrônico ocorre por meio de processos de digitalização, como fotografia, uso de aplicativos específicos ou *scanners*.

Partindo dessa premissa (documento digitalizado # documento digital), no Brasil tem-se a Lei do Processo Judicial Eletrônico (Lei n. 11.419/2006), que dispõe sobre a informatização do processo judicial. Essa lei buscou principalmente promover a emancipação do indivíduo em uma sociedade digital. Conforme explicam Carmen Elisângela Dias Moreira de Resende e outros (2023, p. 145-186), esta lei define como meio eletrônico qualquer forma de armazenamento ou tráfego de documentos e arquivos digitais (inciso I, art. 2º); como transmissão eletrônica, toda forma de comunicação à distância utilizando redes de comunicação, preferencialmente a internet (inciso II, art. 2º); e como assinatura eletrônica, a identificação inequívoca do signatário, seja por certificado digital emitido por Autoridade Certificadora credenciada, conforme legislação específica, ou por cadastro de usuário no Poder Judiciário, conforme regulamentação dos órgãos competentes (inciso III, art. 2º).

Os autores salientam também que o artigo 11 da referida lei estabelece que "os documentos produzidos eletronicamente e anexados aos processos eletrônicos, com garantia de origem e de seu signatário, conforme estabelecido nesta lei, serão considerados originais para todos os efeitos legais" (BRASIL, 2006). Nesse contexto, as provas digitais anexadas aos processos eletrônicos serão consideradas originais para todos os efeitos legais, desde que seja possível verificar sua fonte (RESENDE; BERKENBROCK; RIBEIRO; GOMES; 2023, p. 145-186).

De acordo com o § 3º do artigo 11 da mencionada lei, "os originais dos documentos digitalizados [...] devem ser preservados pelo detentor até o trânsito em julgado da sentença ou, quando permitido, até o final do prazo para interposição de ação rescisória" (BRASIL, 2006) para possibilitar a verificação de sua legitimidade caso haja contestação pela parte adversa. Essa regra é bastante semelhante ao que existia no artigo 225 do Código Civil e no Código de Processo Civil. Assim, a inovação reside em atribuir à parte contrária o ônus da prova quanto à

alegação de falsidade da prova apresentada nos autos, verificando sua autenticidade (RESENDE; BERKENBROCK; RIBEIRO; GOMES; 2023, p. 145-186).

2.3. Autenticidade e integridade da prova e a importância da cadeia de custódia

2.3.1. Autenticidade e integridade da prova

A teoria da prova na era digital enfrenta desafios únicos. A autenticidade e a integridade das provas digitais são questões centrais. Como garantir que um e-mail apresentado como prova não foi adulterado? Como assegurar que uma mensagem de texto é genuína? Essas questões exigem novas abordagens e ferramentas tecnológicas.

A proteção contra ameaças cibernéticas é essencial para garantir a autenticidade e a integridade das provas digitais. Isso inclui a implementação de medidas de segurança robustas, como criptografia e autenticação multifatorial, para proteger dados sensíveis. Isso porque, diferentemente das provas físicas, que podem ser examinadas diretamente, as provas digitais são suscetíveis a manipulações e adulterações. Isso levanta questões críticas sobre como assegurar que um e-mail, uma mensagem de texto ou um arquivo digital não foram alterados desde sua criação.

Isso porque "o documento produzido em meio eletrônico pode, em regra, ser alterado sem esforço, em meios de armazenamento suscetíveis de regravação". Isso se dá porque o "fluxo de dados em uma rede de computadores, como a internet" é muito denso e intenso, fazendo com que "a informação armazenada em meio eletrônico" seja apenas temporária, podendo ser substituída, diante de sua "grande volatilidade" (PASTORE, 2020, p. 64).

Nesse sentido, para que a prova digital alcance o mesmo nível de confiabilidade que a prova documental obtida de um suporte físico, é crucial que ela ofereça a mesma segurança jurídica. Isso só será garantido se forem cumpridas duas condições fundamentais: (i) a origem do documento digital deve ser claramente identificável, assegurando sua autenticidade, o que significa que não deve haver dúvidas sobre quem o produziu; e (ii) deve ser possível verificar a integridade das informações contidas no documento digital, independentemente do formato em que se apresentem, seja texto, áudio, vídeo, entre outros.

Ademais, Guilherme de Siqueira Pastore (2020, p. 68-69) alerta que:

> Vale destacar que tais parâmetros – autenticidade e integridade – são expressamente previstos pela legislação processual para o registro de atos processuais eletrônicos (art. 195 do Código de Processo Civil) e podem ser estendidos, seja por analogia, seja pela própria finalidade da prova, a todo e qualquer registro eletrônico que se pretenda utilizar com força probante no processo.

Nesse sentido, autenticidade refere-se à verificação de que a prova é genuína e não foi falsificada. Isso pode envolver o uso de assinaturas digitais, certificados de autenticidade e registros de metadados. Já a integridade trata da diz respeito à garantia de que a prova não foi modificada. Ferramentas como *hashes* criptográficos e registros de auditoria são frequentemente utilizados para verificar a integridade dos dados digitais.

Na realidade, a doutrina tem destacado que existem três requisitos essenciais — ou pressupostos de validade — para que a prova digital possa ser utilizada com segurança em um processo judicial: (i) a autenticidade; (ii) a integridade; e (iii) a preservação da cadeia de custódia. Assim, é importante compreender o que cada um desses requisitos envolve. Isso porque "A falha em qualquer um desses aspectos resultará na fragilidade da própria prova, tornando-a fraca e, em alguns casos, até mesmo incapaz de produzir efeitos no caso concreto" (THAMAY; TAMER, 2020, p. 39-40).

Dessa forma, Rennan Thamay e Maurício Tamer (2020, p. 40) definem a autenticidade como “a qualidade da prova digital que permite a certeza com relação ao autor ou autores do fato digital”, ou seja, “a qualidade que assegura que o autor aparente do fato é, com efeito, seu autor real” (THAMAY; TAMER, 2020, p. 40).

No que diz respeito à integridade, os mesmos autores esclarecem que é "a característica da prova digital que garante a certeza quanto à sua completude e ausência de adulteração". Assim, a prova digital será considerada íntegra quando se apresentar "livre de qualquer modificação ou adulteração desde o momento da ocorrência do fato até a apresentação do resultado da prova", estando apta a "demonstrar a reprodução do fato em sua totalidade e integridade" (THAMAY; TAMER, 2020, p. 45).

2.3.2. A importância da Cadeia de Custódia

Em relação à cadeia de custódia, trata-se de ponto nevrálgico quanto à validação de provas digitais. Isso porque, conforme destacam Alexandre Morais da Rosa e Aury Lopes Jr. (2015, n.p.), a prova constitui o elemento central do processo penal. É através da prova que se

busca reconhecer um fato ocorrido no passado, permitindo ao juiz tomar, no presente, uma decisão que terá repercussões no futuro.

Dada essa complexidade, e considerando o próprio procedimento de coleta e preservação das provas digitais, torna-se evidente que a observância rigorosa da cadeia de custódia é essencial ao lidarmos com provas digitais (BADARÓ, 2021).

Ademais, conforme destaca Gustavo Badaró (2021, p. 8), "A necessidade de documentação da cadeia de custódia é fundamental para assegurar o potencial epistêmico das fontes de prova reais."

Atualmente, alguns mecanismos são utilizados na cadeia de custódia. Conforme explica Gustavo Badaró (2021, p. 4):

> É imprescindível que o método empregado garanta a integridade do dado digital e, com isso, a força *probandi* do conteúdo probatório por ele representado. Normalmente, faz-se uma cópia ou "espelhamento", obtendo o *bitstream* da imagem do disco rígido ou suporte de memória em que o dado digital está registrado. Além disso, por meio de um cálculo de algoritmo de *hash*, é possível verificar a perfeita identidade da cópia com o arquivo original. Com isso, de um lado, se preserva o material original, e, de outro, se garante a autenticidade e integridade do material que foi examinado pelos peritos.

O autor também pondera que, para assegurar a autenticidade e evitar a contaminação das provas digitais, seria ideal que o legislador definisse uma técnica específica para a individualização e apreensão dessas provas, sob risco de sua inutilização. No entanto, considerando que a informática é uma ciência relativamente jovem, sem métodos e técnicas uniformemente aceitos, e que as técnicas computacionais estão em rápida evolução, essa solução se revela inviável (BADARÓ, 2021, p. 2).

No Brasil, a cadeia de custódia passou a ser legalmente tutelado no Brasil com o advento do pacote anticrime, e se encontra prevista nos artigos 158-A a 158-F, do Código de Processo Penal. Trata-se do mecanismo garantidor de um mínimo de confiabilidade, que documenta o caminho que percorreu a prova, desde a sua coleta, até sua análise pelo juiz competente.

Quando um computador, celular ou qualquer dispositivo similar é submetido a perícia, é fundamental, de acordo com a exigência legal da cadeia de custódia, demonstrar que o objeto analisado é o mesmo que, após a perícia, é apresentado ao juiz. Este é o atual entendimento do Superior Tribunal de Justiça (STJ). Assim, no RHC 143.169/RJ, julgado em 07/02/2023, de relatoria do Min. Messod Azulay Neto, decidiu que "São inadmissíveis as provas digitais, sem

o registro documental acerca dos procedimentos adotados pela polícia para a preservação da integridade, autenticidade e confiabilidade dos elementos informáticos.” (BRASIL, 2023)

Da mesma forma, no julgamento do HC 828.054-RN, julgado em 23/04/2024 e relatado pelo Min. Joel Ilan Paciornik, por unanimidade fixou que “Mostra-se indispensável que todas as fases do processo de obtenção das provas digitais sejam documentadas, cabendo à polícia, além da adequação de metodologias tecnológicas que garantam a integridade dos elementos extraídos, o devido registro das etapas da cadeia de custódia, de modo que sejam asseguradas a autenticidade e a integralidade dos dados.” (BRASIL, 2024)

Como se vê, somente com a adequada documentação da cadeia de custódia da prova conseguir-se-á assegurar sua autenticidade e integralidade, possibilitando o escrutínio da mesma em sede judicial, de modo a preservar a ampla defesa e o contraditório.

3. PRIVACIDADE E SEGURANÇA NA COLETA E NO USO DOS DADOS DIGITAIS

A coleta e o uso de dados digitais levantam preocupações significativas sobre privacidade e segurança. Os operadores do direito devem equilibrar a necessidade de acessar informações relevantes com a proteção dos direitos individuais.

A coleta e o uso de dados digitais são temas que têm ganhado destaque na sociedade contemporânea, principalmente devido ao avanço tecnológico e à crescente digitalização das atividades humanas. Assim, no ambiente digital, é fácil perceber que privacidade e a segurança são pontos sensíveis que merecem destaque. Com a proliferação de dispositivos conectados à internet e a capacidade de armazenar grandes volumes de informações, surgem preocupações significativas sobre como esses dados são coletados, armazenados e utilizados. A privacidade dos indivíduos está em risco quando informações pessoais são capturadas sem consentimento explícito ou quando são utilizadas para fins que os usuários não autorizaram. Além disso, a segurança dos dados é uma questão crítica, pois violações e vazamentos podem expor informações sensíveis, resultando em consequências graves para os indivíduos afetados.

Nesse contexto, enfrenta-se o desafio de equilibrar a necessidade de acessar informações digitais relevantes para investigações e processos judiciais com a proteção dos direitos individuais à privacidade. Este equilíbrio é delicado, pois, por um lado, o acesso a dados pode ser crucial para a resolução de crimes e a administração da justiça. Por outro lado, a coleta

indiscriminada ou excessiva de dados pode levar a abusos e à violação dos direitos fundamentais dos cidadãos.

Em contraste com o mundo digital que experimentamos hoje, Anderson Schreiber (2014, p. 138-139) afirma que o direito à privacidade se expandiu para incluir muito mais do que apenas a proteção de dados pessoais ou o simples direito à intimidade. Daí porque Schreiber define o direito à privacidade como "o direito ao controle da coleta e da utilização dos próprios dados pessoais".

Barreto Junior e Venturini Junior (2020, p. 11-12) fazem analisam a privacidade no contexto do ecossistema digital:

> A privacidade torna-se cada vez mais inatingível na Sociedade da Informação. Perdeu-se, com a tecnologia, a possibilidade de assegurar a diferença entre pessoa identificada e identificável. A dicotomia entre dados anônimos (sigilosos) e dados pessoais, identificáveis não é mais viável em decorrência do aparato tecnológico e das técnicas de *linkage* de bancos de dados, além do georreferenciamento. Inaugura-se um tempo em que os dados pessoais são insumos, uma sociedade movida e orientada por dados.

Na sociedade da informação, os dados pessoais são frequentemente considerados um dos ativos mais valiosos. Eles são utilizados para personalizar serviços, direcionar publicidade e até mesmo para a tomada de decisões automatizadas. No entanto, essa valorização dos dados também os torna alvos atraentes para cibercriminosos, que podem explorar vulnerabilidades em sistemas de segurança para roubar informações sensíveis. Ataques cibernéticos, como *phishing*, *ransomware* e violações de dados, são ameaças constantes que podem ter consequências devastadoras para indivíduos e organizações. Nesse contexto, sobreleva a importância de se garantir a segurança dos dados pessoais.

Analisando essa questão, Denise Francoski e Fernando Tasso (2021, n.p.) aduzem que “a segurança da informação é indissociável da proteção de dados pessoais.”. Explicam, ainda, que embora a garantia da segurança da informação não seja sinônimo do direito à proteção de dados pessoais, como frequentemente se presume, existe uma relação inegável entre ambos. A segurança da informação atua como um pré-requisito essencial, uma condição necessária para que os direitos dos titulares dos dados pessoais sejam efetivamente protegidos (FRANCOSKI, TASSO, 2021, n.p).

Percebe-se, portanto, que é crucial que existam regulamentações claras e rigorosas que orientem a coleta e o uso de dados digitais, garantindo que os direitos dos indivíduos sejam respeitados e que a segurança das informações seja mantida.

No Brasil, a privacidade, como um exemplo dos direitos da personalidade, recebeu atenção especial na Constituição Federal de 1988. No artigo 5º, inciso X, a Constituição declara como invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas (BRASIL, 2024).

Normativos jurídicos têm buscado enfrentar tal problemática. Leis e regulamentos, como o Regulamento Geral sobre a Proteção de Dados [GDPR - Regulamento (EU) 2018/1725] na União Europeia e a Lei Geral de Proteção de Dados (LGPD - Lei n. 13.709/2018) no Brasil, estabelecem diretrizes sobre como os dados pessoais devem ser coletados, armazenados e utilizados. O cumprimento dessas regulamentações é crucial para evitar violações de privacidade (BRASIL, 2024; UNIÃO EUROPEIA, 2018).

Assim, o GDPR da União Europeia unifica e padroniza as regras de tratamento de dados pessoais, ditando como empresas devem coletar, armazenar, proteger e compartilhar informações de cidadãos da UE. A legislação tem alcance extraterritorial, aplicando-se também a empresas fora da UE que ofereçam produtos ou serviços a residentes da União Europeia.

O GDPR tem como objetivo primordial fortalecer a proteção, o controle e a privacidade dos dados pessoais, combatendo sua divulgação indevida. Para se adequarem a essa nova realidade, as empresas precisam realizar uma análise crítica de seus processos e, em muitos casos, implementar mudanças significativas. Ademais, prevê a elaboração de um Plano de Adaptação, que deve ser embasado em um diagnóstico preciso do modelo operacional atual da empresa, mapeando os pontos de atenção e definindo ações concretas a serem implementadas para alcançar a conformidade com o regulamento.

A LGPD, por sua vez, regula o tratamento de dados pessoais, abrangendo informações armazenadas em formato físico ou digital, por entidades públicas ou privadas, independentemente do porte. Essa regulamentação se aplica a uma ampla gama de operações realizadas com os dados, seja por meios manuais ou digitais. O tratamento de dados, ponto central da Lei, engloba qualquer atividade que utilize dados pessoais, desde a coleta até a eliminação. Isso inclui: coleta, produção e recepção (obtenção dos dados, seja diretamente da pessoa ou de outras fontes), classificação, utilização e acesso (organização, uso e consulta das informações), reprodução, transmissão e distribuição (cópia, envio e compartilhamento dos dados), processamento, arquivamento e armazenamento (tratamento, organização e guarda das informações), eliminação, avaliação e controle (exclusão, análise e gestão dos dados),

modificação, comunicação, transferência, difusão ou extração (alteração, compartilhamento, movimentação e divulgação das informações).

Além disso, a transparência e a responsabilidade são princípios fundamentais que devem guiar a atuação dos operadores do direito no contexto digital. As instituições devem adotar práticas que assegurem que os dados sejam coletados de maneira ética e que os indivíduos sejam informados sobre como suas informações estão sendo utilizadas. A implementação de tecnologias de proteção de dados, como criptografia e anonimização, pode ajudar a mitigar riscos e proteger a privacidade dos usuários. Ademais, a educação e a conscientização sobre direitos digitais são essenciais para que os cidadãos possam exercer controle sobre suas informações pessoais e exigir responsabilidade das entidades que as manipulam.

4. EFICIÊNCIA PROCESSUAL E O ACESSO ÀS NOVAS FORMAS DE EVIDÊNCIA

A digitalização das provas e a automação de processos no âmbito jurídico têm o potencial de transformar a eficiência processual. A inserção de tecnologias que automatizam a triagem e a organização de documentos libera os profissionais do direito para concentrarem seus esforços em tarefas mais complexas e estratégicas. Ferramentas digitais, como softwares de gerenciamento de processos e plataformas de armazenamento de dados, permitem que as informações sejam facilmente acessadas e manipuladas, agilizando a coleta e análise de provas. O tempo de resposta, que antes era comprometido por longos processos de busca e organização de documentos físicos, é reduzido. Além disso, a automação minimiza a ocorrência de erros humanos em tarefas repetitivas e aumenta a produtividade.

O professor e magistrado Bruno Alves Rodrigues (2021, p. 183) explica que um dos grandes problemas do poder judiciário fica situado na ocorrência de “gargalos” que prejudicam o impulsionamento dos processos judiciais, o que impacta diretamente no ajuste da tramitação processual com o princípio da duração razoável do processo (art. 5º, LXXVIII, da CF/1988). O autor ainda salienta que atualmente, qualquer empresa moderna possui sistemas operacionais que otimizam o fluxo de processos, enquanto o CPC manteve um sistema que “depende da operação humana, desempenhada pelo escrivão ou chefe de secretaria, para: a) guarda de processos (art. 152, IV, do CPC); b) conclusões (art. 152, IV “a”, do CPC) (...)” (RODRIGUES,

2021, p. 184), sendo que esses sistema analógico com diversas etapas ocasiona a demora no impulsionamento processual, justamente pela necessidade de operação manual.

Assim, utilizando a tecnologia de *analytics*, bem como uma melhor organização e classificação dos processos, influenciaria em uma racionalização maior e sistematização da gestão processual (Rodrigues, 2021, p. 184). Rodrigues (2021, p. 184) ainda traz uma conclusão relevante sobre a questão da identificação dos processos com a sistematização da gestão processual, ainda traz dados importantes sobre os prejuízos sofridos por conta da ausência do monitoramento efetivo dos processos judiciais, confira-se por oportuno:

> Exemplificativamente, poderiam ser identificados processos indevidamente mantidos em 'arquivo', quando pertinente conclusão para análise de hipótese de prescrição intercorrente, ou mesmo para liberação de depósitos judiciais indevidamente mantidos em processos que já contaram com a extinção da execução. Para se ter uma dimensão, por exemplo, do prejuízo causado pela ausência de um monitoramento sistêmico dos depósitos judiciais, apenas na Justiça do Trabalho, no ano de 2020, após o TRT 21 desenvolver o 'Sistema Garimpo', uma ferramenta eletrônica que 'localiza depósitos recursais, honorários periciais e alvarás não sacados por empresas, advogados ou peritos em processos antigos' (LA-GR-PR, 2019), foi identificado 'cerca de R$ 2 bilhões em contas judiciais de empresas e de trabalhadores 'esquecidas' no Banco do Brasil e na Caixa Econômica Federal. Aproximadamente R$ 183 milhões foram liberados após a identificação de seus donos' (NOTÍCIAS DO TST, 2020).

Inegável que o avanço tecnológico com a correta implementação das tecnologias no âmbito jurídico seria capaz de agilizar a tramitação de processos judiciais, resolvendo parte dos problemas com morosidade dentro do poder judiciário como um todo, sendo certo que a "principal baliza ética a ser verificada no desenvolvimento e na implantação de IA no Poder Judiciário é a de jamais permitir que aquilo que necessariamente deva representar expressão de consciência humana seja reduzido à mera manifestação de um ato de inteligência artificial" (RODRIGUES, 2021, p. 186).

É importante ressaltar que a validade jurídica dos documentos eletrônicos não se limita apenas à sua autenticidade e integridade, mas também à sua admissibilidade como prova em processos judiciais. Inclusive, nesse contexto a professora Fernanda Rosa de Vasconcelos Oliveira (2019, p. 19), ressalta que "o meio de armazenamento e a forma de transmissão da informação devem seguir procedimentos seguros capazes de garantir o armazenamento livre de ataques cibernéticos, documentos salvaguardados em repositórios digitais confiáveis – RDC-Arq –, com a segurança de manutenção da cadeia de custódia, assuntos ainda pouco discutidos e com reduzida implementação no país".

Um dos grandes desafios enfrentados pelos operadores do direito na era digital é justamente essa admissibilidade das provas digitais nos tribunais. A volatilidade das provas digitais, que podem ser facilmente manipuladas, levanta dúvidas quanto à sua confiabilidade e integridade. Inicialmente as normas processuais não foram concebidas para lidar com essas características, o que muitas vezes resulta em incertezas sobre a validade das provas apresentadas. Para garantir que as provas digitais sejam admissíveis, as regras precisam ser atualizadas para refletir as particularidades desse novo tipo de prova. Isso inclui, por exemplo, a criação de diretrizes que definam claramente os procedimentos necessários para a coleta, preservação e apresentação de provas digitais.

A questão da coleta, preservação e apresentação das provas digitais, ou seja, a cadeia de custódia da prova é tão relevante, que o Superior Tribunal de Justiça noticiou em 2023 que a quinta turma reconheceu que "são inadmissíveis as provas digitais sem registro documental acerca dos procedimentos adotados pela polícia para a preservação da integridade, da autenticidade e da confiabilidade dos elementos informáticos" (STJ, 2023, online). No caso concreto, o Ministro Ribeiro Dantas, destacou que "antes mesmo de ser periciado pela polícia, o conteúdo extraído dos equipamentos foi analisado pela própria instituição financeira vítima" (STJ, 2023, online).

Além da questão da admissibilidade, a relevância das provas digitais é outro ponto importante, as provas digitais precisam ser analisadas no contexto em que foram criadas e coletadas para determinar sua importância no processo. A facilidade de modificação de provas digitais exige que os advogados realizem uma avaliação da sua relevância e impacto no resultado do caso. Em âmbito penal, a cadeia de custódia, que documenta todos os acessos e movimentações das provas, torna-se o elemento essencial para garantir sua integridade e valor probatório.

Uma solução para essa questão é a utilização de assinaturas digitais e certificados digitais que não apenas fortalece a segurança e confiabilidade dos documentos, mas também facilita sua aceitação como evidência em tribunais e procedimentos legais. Esses mecanismos fornecem uma trilha digital confiável que pode ser auditada e verificada, aumentando a credibilidade dos documentos eletrônicos perante as autoridades judiciárias (OLIVEIRA, 2019, p. 18).

Outro aspecto relevante a considerar quanto ao tema das provas digitais é o desenvolvimento de legislação e regulamentação específica que apoie e valide o uso de documentos eletrônicos na prática jurídica. Em muitos países, foram promulgadas leis e normas que reconhecem a validade legal da assinatura digital e certificação digital, proporcionando um arcabouço jurídico sólido para o uso dessas tecnologias no contexto judicial. Esse reconhecimento legal é fundamental para garantir a segurança jurídica e a eficácia dos documentos eletrônicos em ambientes judiciais.

As leis que reconhecem a validade legal da assinatura digital e certificação digital podem variar de acordo com o país. Nos Estados Unidos, a Lei de Assinaturas Eletrônicas (*E-Sign Act*) e a Lei Uniforme de Transações Eletrônicas (UETA) estabelecem o reconhecimento legal das assinaturas eletrônicas em transações comerciais e legais. No Brasil, a Lei n. 14.063/2020, que dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos, em atos de pessoas jurídicas e em questões de saúde e sobre as licenças de softwares desenvolvidos por entes públicos, também reconhece a validade jurídica da assinatura digital e a classifica como simples, avançada e qualificada, conforme é possível extrair do art. 4º do referido diploma legal[3].

A utilização de técnicas avançadas de criptografia e segurança da informação, por exemplo, permitem a proteção dos documentos eletrônicos contra adulterações e fraudes. A criptografia permite que os dados sejam protegidos contra acessos não autorizados e alterações

[3] Art. 4º Para efeitos desta Lei, as assinaturas eletrônicas são classificadas em:
I - assinatura eletrônica simples:
a) a que permite identificar o seu signatário;
b) a que anexa ou associa dados a outros dados em formato eletrônico do signatário;
II - assinatura eletrônica avançada: a que utiliza certificados não emitidos pela ICP-Brasil ou outro meio de comprovação da autoria e da integridade de documentos em forma eletrônica, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento, com as seguintes características:
a) está associada ao signatário de maneira unívoca;
b) utiliza dados para a criação de assinatura eletrônica cujo signatário pode, com elevado nível de confiança, operar sob o seu controle exclusivo;
c) está relacionada aos dados a ela associados de tal modo que qualquer modificação posterior é detectável;
III - assinatura eletrônica qualificada: a que utiliza certificado digital, nos termos do § 1º do art. 10 da Medida Provisória nº 2.200-2, de 24 de agosto de 2001.
§ 1º Os 3 (três) tipos de assinatura referidos nos incisos I, II e III do caput deste artigo caracterizam o nível de confiança sobre a identidade e a manifestação de vontade de seu titular, e a assinatura eletrônica qualificada é a que possui nível mais elevado de confiabilidade a partir de suas normas, de seus padrões e de seus procedimentos específicos.
§ 2º Devem ser asseguradas formas de revogação ou de cancelamento definitivo do meio utilizado para as assinaturas previstas nesta Lei, sobretudo em casos de comprometimento de sua segurança ou de vazamento de dados.

não autorizadas, garantindo a confidencialidade e integridade das informações contidas nos documentos eletrônicos. Essas medidas de segurança são importantes para mitigar os riscos associados ao uso de documentos eletrônicos na prática jurídica e aumentar a confiança nas tecnologias digitais (INTERNET SOCIETY, 2016, p. 1).

No âmbito da modernização do processo judicial, um escritório de advocacia envolvido em uma disputa civil de propriedade, por exemplo, pode inserir uma variedade de documentos eletrônicos no processo. Isso inclui contratos digitalizados, escrituras públicas e certidões de registro de imóveis pertinentes ao caso. Além disso, e-mails trocados entre as partes ou advogados, contendo acordos prévios ou negociações, podem ser anexados como evidências eletrônicas. Relatórios de avaliação de peritos, transcrições de audiências virtuais e manifestações orais das partes também podem ser documentados eletronicamente para registro no processo. Para garantir a autenticidade e integridade desses documentos, assinaturas digitais e certificados digitais devem ser utilizados, reforçando sua validade jurídica (MENDES; MARQUES, 2021, p. 10).

Nesse contexto, sistemas de inteligência artificial e algoritmos complexos podem ser empregados para auxiliar na tomada de decisões judiciais, promovendo a eficiência processual. Essa abordagem inovadora tem o potencial de revolucionar o sistema judiciário, oferecendo uma alternativa eficiente e ágil para lidar com a crescente demanda por resolução de litígios, o que, conforme mencionado anteriormente, é amplamente ressaltado pelo professor e magistrado Bruno Alves Rodrigues em sua obra, de 2021, “A inteligência Artificial no Poder Judiciário e a Convergência com a consciência humana para a efetividade da justiça”.

Nesse sentido, os professores Juliano Souza de Albuquerque Maranhão, Juliana Abrusio Florêncio e Marco Almada (2021, p. 166), ressaltam que:

> Sistemas baseados em conhecimento são sistemas inteligentes que realizam inferências a partir de representações internas de conhecimento (...). Essas representações do conhecimento são construídas de antemão, durante o projeto de um sistema computacional, mas, uma vez que elas sejam feitas, o sistema pode atualizar sua base de conhecimento a partir das informações que adquire do ambiente, aplicando as mesmas regras de inferência para lidar com situações percebidas.

Assim, é possível concluir que o uso de inteligência artificial (IA) e aprendizado de máquina também é uma inovação que contribui para o aumento da eficiência no âmbito processual. A análise de grandes volumes de dados digitais, realizada por algoritmos avançados, pode identificar padrões, prever resultados e auxiliar advogados e juízes na tomada de decisões mais fundamentadas. A eficiência processual não se resume apenas à redução de tempo, mas

também à melhoria da qualidade das decisões judiciais. As provas digitais, quando integradas a sistemas tecnológicos eficientes, proporcionam uma visão mais abrangente do caso, permitindo a construção de argumentos mais robustos e embasados. No entanto, a eficiência gerada por essas inovações exige um ambiente jurídico adaptado e uma infraestrutura tecnológica robusta, para garantir que as informações sejam manuseadas de forma segura e ágil.

CONCLUSÃO

Os desafios e oportunidades apresentados pela era digital exigem uma adaptação contínua do sistema jurídico. Ao desenvolver novas competências técnicas, garantir a privacidade e a segurança dos dados e aproveitar as tecnologias avançadas, os operadores do direito podem transformar a prática jurídica e melhorar a busca pela justiça. A colaboração entre o direito e a tecnologia será fundamental para enfrentar os desafios e aproveitar as oportunidades que a era digital oferece.

Ao longo deste artigo, ficou evidente que a digitalização dos processos e a proliferação de dados digitais desafiam os conceitos tradicionais de autenticidade, integridade e cadeia de custódia das evidências. Esses desafios exigem do sistema jurídico uma adaptação profunda para garantir que a busca pela verdade processual continue sendo efetiva e justa.

A autenticidade e a integridade das provas digitais emergem como questões centrais neste novo contexto. A facilidade com que dados digitais podem ser alterados ou manipulados demanda a implementação de medidas robustas de segurança cibernética. A utilização de criptografia, autenticação multifatorial e outras tecnologias de proteção torna-se essencial para assegurar que as evidências apresentadas em juízo sejam confiáveis e legítimas.

A importância da cadeia de custódia é reforçada na era digital, pois ela garante a rastreabilidade e a confiabilidade das provas desde a sua coleta até a apresentação. Sem um controle rigoroso dessa cadeia, a admissibilidade das provas digitais pode ser comprometida, afetando diretamente a tomada de decisões judiciais. Portanto, protocolos claros e padronizados para o manuseio de evidências digitais são indispensáveis.

A privacidade e a segurança na coleta e uso de dados digitais também se apresentam como preocupações, tornando necessário equilibrar o acesso a informações relevantes para a justiça com a proteção dos direitos individuais. A legislação e as práticas jurídicas precisam

evoluir para garantir que a coleta de dados não infrinja direitos fundamentais, mantendo a integridade do processo legal.

A digitalização traz, ainda, oportunidades significativas para a eficiência processual. A automação de tarefas e o uso de inteligência artificial podem agilizar procedimentos, reduzir erros e aprimorar a análise de grandes volumes de dados. No entanto, a adoção dessas tecnologias requer investimentos em infraestrutura e formação adequada dos profissionais do direito, garantindo que estejam aptos a lidar com as novas ferramentas.

Assim, destaca-se a necessidade de uma formação interdisciplinar para os operadores do direito. A colaboração com especialistas em tecnologia torna-se cada vez mais relevante, e a educação jurídica deve incorporar conhecimentos técnicos em seus currículos. Somente assim será possível enfrentar os desafios da era digital e aproveitar plenamente as oportunidades que ela oferece.

Em suma, a digitalização impõe uma reconfiguração da Teoria da Prova e das práticas processuais. Cabe ao sistema jurídico adaptar-se de maneira proativa, promovendo mudanças que assegurem a efetividade, a segurança jurídica e a proteção dos direitos fundamentais na era da informação, sendo certo que o futuro da justiça depende da capacidade de integrar a tecnologia de forma ética e eficiente em seus procedimentos.

REFERÊNCIAS

BADARÓ, Gustavo. A cadeia de custódia da prova digital. Artigo elaborado para apresentação de palestra, como mesmo tema, no **Congresso Internacional de Direito Probatório**, realizado nos dias 18 e 19 de novembro de 2021, em Porto Alegre-RS, pela Pontifícia Universidade Católica do Rio Grande do Sul e pela Universidade Alberto Hurtado, com apoio do IBDP e da Procnet. Disponível em: https://edisciplinas.usp.br/pluginfile.php/7833426/mod_resource/content/1/U8%20-%20BADARO%20-%20A%20cadeia%20de%20custo%CC%81dia%20da%20prova%20digital%20PUCRS%20-%20co%CC%81pia.pdf. Acesso em: 19 out.2024.

BARRETO JUNIOR, Irineu Francisco; VENTURINI JUNIOR, Gustavo. Inteligência Artificial e seus efeitos na Sociedade da Informação. *In*: LISBOA, Roberto Senise (Org.). **O Direito na Sociedade da Informação.** v.4, 2020. São Paulo (SP): Almedina, 2020.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 19 out.2024.

BRASIL. Decreto-lei n. 3.689, de 3 de outubro de 1941. **Código de Processo Penal (CPP)**. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em: 19 out.2024.

BRASIL. Lei 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados (LGPD)**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 19 out. 2024.

BRASIL. Lei n. 11.419, de 19 de dezembro de 2006. **Lei do Processo Eletrônico**. Dispõe sobre a informatização do processo judicial. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/L11419.htm. Acesso em: 19 out. 2024.

BRASIL. **Superior Tribunal de Justiça**. AgRg no HABEAS CORPUS Nº 828054 - RN (2023/0189615-0). Ministro Relator Joel Ilan Paciornik. Quinta Turma. Julgado em 23/04/2024. Disponível em: https://processo.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202301896150&dt_publicacao=29/04/2024. Acesso em 19 out.24.

BRASIL. **Superior Tribunal de Justiça**. AgRg no RECURSO EM HABEAS CORPUS Nº 143.169 - RJ (2021/0057395-6). Ministro Relator Jesuíno Rissato (Desembargador Convocado do TJDFT). Julgado em 07/02/2023. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202100573956&dt_publicacao=02/03/2023. Acesso em: 19 out.2024.

BRASIL. Superior Tribunal de Justiça. **A cadeia de custódia no processo penal: do Pacote Anticrime à jurisprudência do STJ**. Publicado em 23 de abril de 2023. Online. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2023/23042023-A-cadeia-de-custodia-no-processo-penal-do-Pacote-Anticrime-a-jurisprudencia-do-STJ.aspx. Acesso em: 21 out.2024.

BRASIL. Lei n. 11.419, de 19 de dezembro de 2006. **Lei do Processo Eletrônico**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11419.htm. Acesso em: 09 dez. 2024.

BRASIL. Lei n. 14.063, de 23 de setembro de 2020. **Dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos, em atos de pessoas jurídicas e em questões de saúde e sobre as licenças de softwares desenvolvidos por entes públicos**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l14063.htm. Acesso em: 09 dez. 2024.

BUENO, Cassio Scarpinella. **Curso sistematizado de direito processual civil**. v. 02, tomo I, 3. ed. São Paulo (SP): Saraiva, 2010.

CASTELLS, Manuel. **A sociedade em rede – a era da informação: economia, sociedade e cultura**. Tradução: Roneide Venâncio Majer, com a colaboração de Klauss Brandini Gerhardt. Atualização para a 6. ed.: Jussara Simões. 6. ed. ver. e ampl. São Paulo: Paz e Terra, 1999, p. 39-40.

FRANCOSKI, Denise; TASSO, Fernando. Capítulo 20. Segurança da Informação e Proteção de Dados Pessoais. *In*: FRANCOSKI, Denise; TASSO, Fernando. **A Lei Geral de Proteção de Dados Pessoais: LGPD: Aspectos Práticos e Teóricos Relevantes no Setor Público e Privado**. São Paulo (SP): Editora Revista dos Tribunais. 2021. Disponível em: https://www.jusbrasil.com.br/doutrina/secao/capitulo-20-seguranca-da-informacao-e-protecao-de-dados-pessoais-parte-i-a-lei-geral-de-protecao-de-dados-pessoais-no-setor-publico/1279975775?utm_source=google&utm_medium=cpc&utm_campaign=doutrina_dsa&utm_term=&utm_content=capitulos&campaign=true&gad_source=1&gclid=Cj0KCQjwsc24BhDPARIsAFXqAB1NrC6WonsducWUV44eld-hZWQiYqAgDMFf1MZGEJR8SWNm1vh5UVcaAg3PEALw_wcB#ftn.DTR.2021.7724-n2. Acesso em: 19 out.2024.

INTERNET SOCIETY. **Criptografia**. Disponível Em: https://www.internetsociety.org/wp-content/uploads/2016/06/ISOC-PolicyBrief-Encryption-Portuguese.pdf. Acesso em: 23 out.2024.

JANINI, Tiago Cappi. O documento eletrônico como meio de prova no Direito Tributário. *In*: **Direito Tributário Eletrônico**. Coord. Maria Rita Ferrogut. Colab. Renata Elaine Silva. São Paulo: Saraiva, 2010.

KIST, Dário José. **Prova Digital no Processo Penal**. 2. ed., Leme (SP): Mizuno, 2024.

LOPES JUNIOR, Aury; ROSA, Alexandre Morais da. A importância da cadeia de custódia para preservar a prova penal. **Consultor Jurídico (Conjur)**, publicado em 16 de janeiro de 2015 às 7h00. Disponível em: Disponível em: https://www.conjur.com.br/2015-jan-16/limite-penal-importancia-cadeia-custodia-prova-penal/. Acesso em: 19 out.2024.

LUCIEN, Lucien Rocha. **Acreditação e admissibilidade de evidências digitais de crimes cibernéticos praticados em computação de nuvem: desafios na esfera judicial do Brasil.** Dissertação (Mestrado em Direito). Universidade de Brasília – UNB. Brasília. 2023.

MARANHÃO, Juliano Souza De Albuquerque; FLORÊNCIO, Juliana Abrusio; ALMADA Marco. Inteligência Artificial Aplicada ao Direito e o Direito da Inteligência Artificial. **Suprema - Revista de Estudos Constitucionais**, v. 1, n. 1, 2021, p. 154-180. Disponível em: https://suprema.stf.jus.br/index.php/suprema/article/view/20. Acesso em: 23 out.2024.

MARINONI, Luiz Guilherme; MITIDIERO, Daniel. **Código de processo civil comentado**. São Paulo (SP): Revista dos Tribunais, 3. ed., 2011.

MENDES, Josilene Maria Aparecida De Paula; MARQUES, João Victor Mota. **Modernização Tecnológica Do Processo Judicial No Brasil**. 2021. Disponível em: Acesso em: 23 out.2024.

OLIVEIRA, Fernanda Rosa de Vasconcelos. A Força Probante dos Documentos Digitalizados: Eficiência Versus Segurança Jurídica. **Revista Caderno Virtual**, 2019. Disponível em: https://www.portaldeperiodicos.idp.edu.br/cadernovirtual/article/view/4166. Acesso em: 21 out.2024.

PASTORE, Guilherme de Siqueira. Considerações sobre a autenticidade e a integridade da prova digital. **Cadernos Jurídicos**, São Paulo (SP), ano 21, n. 53, p. 63-79, jan./mar. 2020.

RESENDE, Carmen Elisângela Dias Moreira de.; BERKENBROCK, Guy Estevão; RIBEIRO, Luiz Octávio O. Saboia; GOMES, Magáli Dellape. **Revista Judicial Brasileira (ReJuB)**, Ed. esp. Direito Digital, Brasília (DF), p. 145-186, jul./dez. 2023.

RODRIGUES, Bruno Alves. **A inteligência artificial no poder judiciário e a convergência com a consciência humana para a efetividade da justiça**. São Paulo: Thomson Reuters Brasil, 2021.

ROSA, Alexandre Morais da. Limite Penal: o *"print screen"* é insuficiente à materialidade nos crimes digitais. **Consultor Jurídico (Conjur)**, publicado em 17 de junho de 2022, 15h44. Disponível em: https://www.conjur.com.br/2022-jun-17/limite-penal-print-screen-materialidade-crimes-digitais/. Acesso em: 19 out.2024.

SCHREIBER, Anderson. **Direitos da Personalidade**. 3. ed. São Paulo: Atlas, 2014.

THAMAY, Rennan; TAMER, Maurício. **Provas no Direito Digital**. São Paulo (SP): Editora Revista dos Tribunais. 2022. Disponível em: https://www.jusbrasil.com.br/doutrina/provas-no-direito-digital-ed-2022/1672935656. Acesso em: 16 out.2024.

THAMAY, Rennan; TAMER, Mauricio. **Provas no direito digital: conceito da prova digital, procedimentos e provas digitais em espécie**. São Paulo/SP: Thomson Reuters Brasil, 2020.

UNIÃO EUROPEIA (EU). Parlamento Europeu. **Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018**, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n. 45/2001 e a Decisão n. 1247/2002/CE. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32018R1725#:~:text=Regulamento%20(UE)%202018%2F1725,o%20Regulamento%20(CE)%20n. Acesso em: 19 out.2024.

7 Information Society and Law
FMU CENTRO UNIVERSITÁRIO

SOCIEDADE DA INFORMAÇÃO E OS NOVOS PARADIGMAS DO DIREITO: CRIMES CIBERNÉTICOS, PRIVACIDADE E ACESSO À INFORMAÇÃO

INFORMATION SOCIETY AND THE NEW PARADIGMS OF LAW: CYBERCRIME, PRIVACY, AND ACCESS TO INFORMATION

Edielma Rocha Dutra[1]; Kelly Cristina Maciel da Silva Costa[2]

RESUMO: Este artigo propõe uma análise abrangente dos desafios enfrentados pela Sociedade da Informação no combate aos crimes cibernéticos, delineando estratégias cruciais para enfrentar essa problemática complexa. Ao examinar as legislações pertinentes e os obstáculos enfrentados na investigação desses delitos, destaca-se a necessidade de uma abordagem integrada que envolva o Direito, a tecnologia e a sociedade. Nesse contexto, são exploradas soluções como o aprimoramento da legislação específica, o investimento em capacitação das autoridades e a promoção da conscientização social. Além disso, ressalta-se a importância de encontrar um equilíbrio entre o direito à privacidade e à informação, fundamentais para o exercício da cidadania e o fomento ao debate democrático. Por meio dessa análise, busca-se contribuir para a construção de um ambiente digital mais seguro e ético, capaz de enfrentar os desafios impostos pelos crimes cibernéticos na contemporaneidade.
Palavras-chave: crimes cibernéticos; Sociedade da Informação; conscientização social; privacidade e informação.

ABSTRACT: This article proposes a comprehensive analysis of the challenges faced by the Information Society in combating cybercrimes, outlining crucial strategies to address this complex issue. By examining relevant legislations and the hurdles encountered in investigating these offenses, the need for an integrated approach involving Law, technology, and society is underscored. In this context, solutions such as enhancing specific legislation, investing in

[1] Oficial de Promotoria no Ministério Público do Estado de São Paulo (MPSP). Graduada pela Universidade Católica de Santos (UNISANTOS). Pós-graduada em Direito Processual Penal pela Instituto Damásio de Direito/IBMEC. Pós-graduanda em Direito Penal e Criminologia na PUC - Rio Grande do Sul. Mestranda em Direito da Sociedade da Informação nas Faculdades Metropolitanas Unidas.
[2]Advogada e membro efetivo da Comissão de Privacidade e Proteção de Dados da OAB-SP. Membro do Núcleo Docente Estruturante - NDE das Faculdades Metropolitanas Unidas - FMU, nos cursos de Sistemas de Informação, Big Data e Inteligência Analítica, Jogos Digitais, Análise e Desenvolvimento de Sistemas, Sistemas para Internet, Bacharelado em Ciência da Computação, Gestão da Tecnologia da Informação. Apoio à Coordenação dos Cursos de Tecnologia da Informação da FMU. Professora Universitária nos cursos de Engenharia de Controle e Automação, Bacharelado em Ciência da Computação, Análise e Desenvolvimento de Sistemas e Sistemas da Informação. Mestra e Doutoranda em Engenharia da Informação na Universidade Federal do ABC - UFABC. Mestranda em Direito da Sociedade da Informação na FMU; bolsista integral pela própria instituição. Bacharela em Direito pela Universidade Paulista - UNIP (jun/2022); bolsista integral pela própria instituição. Bacharela em Engenharia de Controle e Automação pela Universidade Paulista - UNIP (dez/2016); bolsista integral pelo programa PROUNI. Estudante do curso de Bacharelado em Ciência e Tecnologia da UFABC. E-mail: kellymacielcosta@gmail.com / kelly.maciel@aluno.ufabc.edu.br.

authorities' training, and promoting social awareness are explored. Moreover, the importance of striking a balance between the right to privacy and information, fundamental for citizenship exercise and fostering democratic debate, is emphasized. Through this analysis, the aim is to contribute to building a safer and more ethical digital environment capable of tackling the challenges posed by cybercrimes in contemporary times.
Keywords: cybercrimes; Information Society; social awareness; privacy, and information.

INTRODUÇÃO

A Sociedade da Informação, impulsionada pelo desenvolvimento das tecnologias de informação e comunicação (TICs), trouxe consigo profundas transformações nas relações sociais, econômicas e políticas em todo o mundo. Se, por um lado, essas tecnologias proporcionaram inúmeros benefícios, como a facilidade de acesso à informação, a comunicação instantânea e a globalização dos mercados, por outro, também, criaram desafios e riscos, especialmente no âmbito do Direito.

Entre esses desafios, destacam-se os crimes cibernéticos, que se aproveitam das vulnerabilidades e da sensação de anonimato proporcionada pela internet para a prática de condutas ilícitas, como a invasão de sistemas, a disseminação de malware, as fraudes eletrônicas e a violação de direitos autorais.

Esses crimes, por sua natureza transnacional e sua complexidade técnica, têm exigido um constante aprimoramento das legislações e das estratégias de prevenção e repressão por parte dos Estados e da comunidade internacional.

Além disso, a Sociedade da Informação também tem suscitado intensos debates sobre o equilíbrio entre o direito à privacidade e o direito à informação. Com a crescente coleta, armazenamento e processamento de dados pessoais por empresas e governos, surgem preocupações legítimas sobre a proteção da privacidade e da autodeterminação informativa dos indivíduos.

Ao mesmo tempo, a necessidade de acesso a determinadas informações para a investigação e punição de crimes cibernéticos tem gerado conflitos e questionamentos sobre os limites e as condições para a quebra de sigilo de dados.

Nesse contexto, este artigo tem como objetivo analisar esses desafios, com a finalidade de compreender as implicações jurídicas da Sociedade da Informação e propor soluções que

possam equilibrar os benefícios proporcionados pelas tecnologias emergentes com a proteção dos direitos fundamentais.

Para isso, serão abordados três principais eixos de discussão: a regulação dos crimes cibernéticos, a proteção da privacidade e dos dados pessoais, e a promoção de uma governança global da internet.

Para tanto, foi realizada uma pesquisa bibliográfica e documental, buscando identificar os principais conceitos, teorias e discussões relacionados ao tema, bem como o marco legal e regulatório aplicável em âmbito nacional e internacional.

Esta revisão literária demonstrou a complexidade e a relevância dos temas abordados, fornecendo as bases teóricas e conceituais para a análise dos crimes cibernéticos e do equilíbrio entre privacidade e informação na Sociedade da Informação.

Foram abordados os principais tipos de crimes cibernéticos, os desafios relacionados à sua prevenção e repressão, além das respostas legislativas e regulatórias tanto em âmbito nacional quanto internacional.

Destaque especial foi dado à Convenção de Budapeste sobre o Cibercrime e à Lei Geral de Proteção de Dados (LGPD) no Brasil.

Também foram analisados os conflitos entre o direito à privacidade e o direito à informação, ressaltando a importância da proteção de dados pessoais e da autodeterminação informativa, assim como os desafios enfrentados na investigação e punição dos crimes cibernéticos.

Por fim, foram discutidos os desafios da liberdade de expressão e do anonimato na internet, analisando-se sua importância para a democracia e a inovação, mas também seus potenciais riscos e abusos.

Foram apresentadas as principais diretrizes internacionais sobre o tema, como a Declaração Conjunta sobre Liberdade de Expressão e Internet, bem como as discussões doutrinárias sobre os limites e as condições para o exercício desses direitos no ambiente digital.

Espera-se que este artigo possa contribuir para o aprofundamento das reflexões sobre os impactos da Sociedade da Informação no Direito, fornecendo subsídios para o aprimoramento das respostas jurídicas e políticas a essas questões. Somente com um esforço conjunto e multidisciplinar será possível construir um ambiente digital mais seguro, justo e democrático para todos.

1. SOCIEDADE DA INFORMAÇÃO

Manuel Castells (2018, p. 108-109) em sua obra "Sociedade em Rede", define que a atual Sociedade da Informação é caracterizada por um paradigma da tecnologia da informação. Segundo o autor, este paradigma é guiado por eventos específicos que consideram a informação como matéria prima, a alta convergência tecnológica e a topologia em rede da difusão de informação. Christopher Freeman e Luc Soete (1982, p. 14-16), economista focado na inovação e no desenvolvimento econômico e científico, define o paradigma tecnológico como a combinação de inovações técnicas, administrativas e organizacionais inter-relacionadas, cujas vantagens são amplamente aplicáveis. Esse paradigma não apenas afeta a variedade de produtos disponíveis em um dado momento, mas também a dinâmica dos custos de produção.

O advento da Sociedade da Informação marca uma mudança fundamental na maneira como as economias e as sociedades funcionam. Com a informação como matéria-prima principal e a alta convergência tecnológica, os processos econômicos, sociais e culturais são profundamente influenciados. Essa era é caracterizada pela interconexão global e pela disseminação instantânea de informações, possibilitada pela infraestrutura digital e pela internet.

Essa interconexão global e a disseminação instantânea de informações na Sociedade da Informação estão intrinsecamente ligadas aos efeitos da globalização. A globalização, impulsionada em grande parte pela revolução digital, redefine as relações econômicas, culturais e políticas entre as nações. A capacidade de comunicação instantânea e o acesso a vastas quantidades de informações em tempo real transcendem as fronteiras físicas, permitindo uma integração mais profunda das economias e das culturas em escala mundial.

Nesse contexto, as empresas podem operar em múltiplos mercados simultaneamente, aproveitando os avanços tecnológicos para coordenar cadeias de suprimentos globais e alcançar consumidores em qualquer lugar do mundo. Essa interconexão econômica cria oportunidades para o crescimento e a prosperidade, mas também traz desafios, como a competição acirrada e a necessidade de adaptação a diferentes contextos culturais e regulatórios.

Além disso, a globalização da informação e da cultura tem impactos significativos na sociedade. Por um lado, ela facilita o intercâmbio de ideias e valores, promovendo a compreensão intercultural e o desenvolvimento de uma consciência global. Por outro lado,

levanta questões sobre a homogeneização cultural e a perda de identidade cultural em face da influência dominante de certas narrativas e produtos midiáticos.

A perspectiva da informação como matéria-prima é uma das características fundamentais da Sociedade da Informação. Nesse paradigma, a informação é vista como um recurso valioso e essencial para o funcionamento da economia e da sociedade em geral. Assim como a matéria-prima tradicional, como minerais e recursos naturais, a informação é um elemento fundamental para a produção de bens e serviços, bem como para a tomada de decisões em todos os níveis.

Essa visão da informação como matéria-prima destaca sua importância econômica e estratégica. Empresas e organizações buscam cada vez mais capturar, processar e utilizar informações de maneira eficaz para ganhar vantagem competitiva, inovar e atender às necessidades dos clientes. Da mesma forma, governos e instituições públicas reconhecem o valor da informação para orientar políticas públicas, planejamento urbano, gestão de recursos e tomada de decisões em geral.

A digitalização e a tecnologia da informação desempenham um papel crucial nesse contexto, tornando mais fácil e rápido o acesso, o armazenamento e o compartilhamento de grandes volumes de informações. A infraestrutura digital, como a internet e as redes de comunicação, cria uma plataforma global que permite a troca instantânea de dados e conhecimentos em escala sem precedentes.

No entanto, a perspectiva da informação como matéria-prima também levanta questões importantes relacionadas à privacidade, segurança e controle. O aumento da coleta e do uso de informações pessoais e comerciais levanta preocupações sobre o uso ético e responsável dos dados, bem como sobre a proteção contra ameaças cibernéticas e violações de segurança.

Por outro lado, a alta convergência tecnológica é outro aspecto crucial da Sociedade da Informação, e está intimamente ligada à perspectiva da informação como matéria-prima. Esse fenômeno refere-se à tendência de diferentes tecnologias convergirem e se fundirem, criando possibilidades e sinergias entre elas. Esta convergência é demarcada pela integração de tecnologias digitais, como a internet, a computação em nuvem, a inteligência artificial, a Internet das Coisas (IoT), a realidade aumentada (AR) e virtual (VR), entre outras. Essas tecnologias emergentes não apenas coexistem, mas também interagem e se complementam, criando um ecossistema tecnológico cada vez mais integrado e interconectado.

Essa alta integração tecnológica tem profundas implicações na forma da comunicação, aprendizagem e interação da sociedade. No entanto, esse fenômeno também traz desafios, como questões de segurança cibernética, privacidade de dados e desigualdades digitais. À medida que as tecnologias convergem e se tornam cada vez mais interdependentes, a complexidade e o potencial de vulnerabilidades aumentam, exigindo uma abordagem cuidadosa e colaborativa para mitigar riscos e garantir que os benefícios da inovação tecnológica sejam amplamente compartilhados.

A abordagem de Castells (2018, p.108) também destaca a importância da topologia em rede na difusão da informação. As redes de comunicação e de dados são os principais facilitadores da troca rápida e global de informações, permitindo a interconexão entre pessoas, organizações e dispositivos em todo o mundo. Nesse contexto, a velocidade da transmissão de informações e a capacidade de processamento se tornam fatores-chave na determinação do sucesso econômico e social.

A topologia em rede da difusão de informação é outro aspecto essencial da Sociedade da Informação. Essa abordagem reconhece que a disseminação de informações na era digital não segue mais modelos unidirecionais ou centralizados, mas sim se baseia em redes complexas e interconectadas.

Nesse diapasão, a informação flui por meio de uma variedade de canais e plataformas, muitas vezes de forma descentralizada e sem uma autoridade central que controle ou dirija o fluxo. Isso significa que as informações podem se espalhar rapidamente e alcançar públicos globais em questão de segundos, graças às redes de comunicação digitais, como a internet e as mídias sociais.

A natureza em rede da difusão de informações tem implicações profundas em várias áreas. Por um lado, isso democratiza o acesso à informação, permitindo que indivíduos e comunidades compartilhem conhecimentos e perspectivas de maneira mais ampla e inclusiva. Por outro lado, também cria desafios relacionados à confiabilidade e à veracidade das informações, uma vez que notícias falsas e desinformação podem se espalhar tão rapidamente quanto informações legítimas.

Além disso, a topologia em rede da difusão de informação está transformando a natureza do poder e da influência na sociedade. Em vez de depender de fontes tradicionais de autoridade, como governos ou instituições de mídia, indivíduos e grupos podem agora exercer

influência por meio de redes sociais e plataformas online, conectando-se diretamente com audiências globais e mobilizando apoio para causas e ideias.

No entanto, essa topologia em rede também levanta preocupações sobre questões como privacidade, segurança cibernética e regulação de conteúdo online. A natureza descentralizada e distribuída da difusão de informação torna mais difícil controlar e regular o fluxo de informações, criando desafios para a proteção de dados pessoais e o combate a abusos online.

Por outro lado, a visão de Freeman e Soete (1982, p. 14-16), sobre o paradigma tecnológico ressalta a interdependência entre inovações técnicas, administrativas e organizacionais. Esse paradigma impulsiona o desenvolvimento econômico ao criar vantagens competitivas por meio da aplicação de novas tecnologias e práticas organizacionais. Como resultado, as economias que conseguem adotar e adaptar-se rapidamente a essas inovações são mais propensas a prosperar na Sociedade da Informação.

Nesse contexto, as empresas e as economias que conseguem adotar e adaptar-se rapidamente a essas inovações têm uma vantagem significativa. Ao implementar novas tecnologias e práticas organizacionais de forma eficaz, elas podem aumentar a eficiência, reduzir os custos de produção, melhorar a qualidade dos produtos e serviços e responder de maneira mais ágil às mudanças no ambiente de negócios.

Essa capacidade de adaptação e inovação é especialmente importante na Sociedade da Informação, onde a tecnologia está em constante evolução e a concorrência é global. As economias que conseguem acompanhar o ritmo das mudanças tecnológicas estão mais bem posicionadas para prosperar, aproveitando as oportunidades oferecidas por essa era de rápida transformação e disrupção.

No entanto, a adoção de novas tecnologias e práticas organizacionais também pode apresentar desafios, especialmente para empresas e setores que enfrentam resistência à mudança ou que têm estruturas organizacionais rígidas e processos estabelecidos. Nesses casos, a capacidade de adaptação pode ser limitada, tornando essas empresas mais suscetíveis a ficarem para trás ou mesmo a serem obsoletas no mercado.

Assim, Castells (2018, p.108-109) e Freeman e Soete (1982, p. 14-16), oferecem *insights* valiosos sobre a natureza e as implicações do paradigma tecnológico na era da Sociedade da Informação. Enquanto o primeiro destaca a importância da interconexão e da difusão de informações em rede, o segundo enfatiza a necessidade de inovação e adaptação para

aproveitar ao máximo as oportunidades oferecidas por esse novo paradigma. Juntos, esses conceitos ajudam a compreender melhor os desafios e as oportunidades enfrentados pelas sociedades contemporâneas em meio à rápida evolução tecnológica.

Alguns outros autores, como Pierre Lévy (2021, p. 21-31), enfatizam o papel da cibercultura e da inteligência coletiva na Sociedade da Informação, ressaltando as potencialidades e os desafios éticos e políticos da virtualização das relações humanas.

Nesse sentido, Lévy enfatiza o papel da cibercultura e da inteligência coletiva na Sociedade da Informação, destacando as potencialidades e os desafios éticos e políticos da virtualização das relações humanas.

Lévy (2021, p. 21-31) explica que a cibercultura deve ser entendida como o conjunto de práticas, valores e modos de pensamento que emergem no ciberespaço, possui o potencial de fomentar novas formas de colaboração, criatividade e compartilhamento de conhecimentos.

Lévy (2021, p. 27), define que "a velocidade de transformação é em si mesma uma constante - paradoxal - da cibercultura". Ademais, define que a inteligência coletiva é um dos principais motores da cibercultura (Lévy, 2021, p. 28), que se refere à capacidade das comunidades virtuais de mobilizar competências e recursos para resolver problemas complexos e gerar inovações de maneira distribuída e colaborativa.

Ademais, Lévy (2021, p. 46) examina o impacto da virtualização e a considera como um "traço distintivo da nova face da informação". Define também que "a digitalização é o fundamento técnico da virtualidade". Nest sentido, classifica que a cibercultura encontra-se ligada ao virtual direta e indiretamente (Levy, 2021, p. 48).

Por outro lado, Benkler (2021, p. 457) dedicou inteiramente a obra ao surgimento da produção de informações baseadas em bens comuns e suas consequências para as democracias liberais. O autor observa que, impulsionadas pela mudança tecnológica, estão surgindo adaptações econômicas, sociais e culturais que possibilitam uma transformação significativa na forma como se cria o ambiente de informação.

Esse novo contexto permite que os indivíduos atuem de maneira mais autônoma, exercendo seu papel como cidadãos e membros de grupos culturais e sociais, redefinindo as bases da produção e compartilhamento de conhecimento (Benkler, 2021, p. 1).

Quanto ao tema da privacidade, importante mencionar a obra de Stefano Rodotà (2021), que apresenta uma série de problemas concretos do grande público e evidencia uma necessidade de a convocar a atenção de todos para a sua resolução.

Rodotà demonstra grande lucidez ao buscar soluções viáveis para os conflitos gerados pelas novas tecnologias, soluções que, além de serem tecnicamente eficazes, também respeitem a dignidade da pessoa humana e os princípios fundamentais da democracia. Ele procura equilibrar a inovação tecnológica com a necessidade de proteger os direitos e liberdades dos indivíduos, garantindo que o progresso não comprometa os valores essenciais da sociedade (RODOTÀ, 2021).

O autor analisa a evolução do conceito de privacidade e sua relação com a autodeterminação informativa, destacando a necessidade de um novo quadro jurídico para a proteção dos dados pessoais. Para ele, a evolução do conceito de privacidade traz consigo o sentido de relação com a autodeterminação informativa na era digital.

Conforme analisa, a crescente coleta, processamento e uso de dados pessoais requer um novo quadro jurídico capaz de proteger os direitos fundamentais dos indivíduos. Ademais, o autor destaca a necessidade de garantir aos cidadãos o controle sobre suas informações pessoais, permitindo que eles decidam como e quando seus dados podem ser utilizados.

Nesse contexto, Rodotà em sua obra defende a atualização das leis de proteção de dados, a fim de assegurar a transparência, a *accountability* e a participação dos indivíduos nos processos de tratamento de suas informações (RODOTÀ, 2021).

Além disso, ele ressalta a importância de equilibrar a proteção da privacidade com outros valores democráticos, como a liberdade de expressão e o acesso à informação, buscando soluções que promovam a dignidade humana e a autodeterminação na sociedade da informação.

Outros autores que contribuem para a temática em suas obras são Danilo Doneda (2021) e Laura Schertel Mendes (2014). Nesse sentido, ambos abordam a proteção de dados pessoais no contexto jurídico brasileiro. O autor analisa os fundamentos dessa proteção no ordenamento jurídico do país, traçando a evolução legislativa e jurisprudencial sobre o tema.

Define que a tendência, que pode ser descrita como uma "força expansiva" na proteção de dados pessoais, vai além de ser uma simples característica intrínseca dos chamados "novos direitos"; manifesta-se na própria transformação do ambiente em que os dados circulam e no qual se expressam os interesses relacionados à privacidade (Doneda, 2021, p.91)

Já Mendes (2014, p. 37-44) traz diversos temas relacionados à privacidade e proteção de dados, trazendo uma reflexão sobre o desenvolvimento geracional das leis direcionadas para este tema e sobre o regime jurídico de proteção de dados pessoais. A autora analisa as principais disposições desses instrumentos legais, destacando seus pontos fortes e fracos, bem como as dificuldades de implementação no contexto brasileiro.

No âmbito internacional, tem-se os autores como Paul de Hert e Serge Gutwirth (2021). Ambos analisam a evolução da proteção de dados pessoais como um direito fundamental na União Europeia, enfatizando o papel crucial do Regulamento Geral sobre a Proteção de Dados (GDPR) nesse processo. Os autores argumentam que o GDPR representa um marco na harmonização legislativa e na efetivação do direito à proteção de dados pessoais no âmbito europeu, estabelecendo um conjunto abrangente e robusto de normas e princípios.

Os autores destacam, ainda, que o regulamento fortaleceu os direitos dos titulares de dados, impôs obrigações mais rigorosas aos controladores e processadores de dados, e criou mecanismos de aplicação/cumprimento internacional (estes conceitos são a tradução do famoso termo “enforcement internacional", em que, no contexto da proteção de dados pessoais, o termo se refere aos mecanismos e práticas utilizados para garantir que as normas e regulamentos de proteção de dados sejam efetivamente aplicados e cumpridos em um âmbito internacional, ou seja, além das fronteiras de um único país) e sanções significativas.

Assim, De Hert e Gutwirth (2021) ressaltam que o GDPR se tornou uma referência global para a regulação da proteção de dados pessoais, influenciando a legislação de outros países e regiões do mundo. Os autores concluem que o GDPR desempenha um papel fundamental na consolidação da proteção de dados pessoais como um direito fundamental na era digital, contribuindo para o fortalecimento da privacidade e da autodeterminação informativa dos indivíduos na União Europeia.

Outro importante autor para a temática é Christopher Kuner (2021). Nesse sentido, Kuner aborda os desafios da regulação transnacional da proteção de dados pessoais, destacando a necessidade de mecanismos de cooperação e, da mesma forma, chama a atenção da importância da aplicação internacional.

O autor argumenta que, em um contexto de fluxos de dados globais, é essencial desenvolver instrumentos e práticas que assegurem a aplicação efetiva das normas de proteção de dados além das fronteiras nacionais.

Ademais, Kuner enfatiza a importância da colaboração entre autoridades reguladoras de diferentes países, por meio de acordos bilaterais e multilaterais, para lidar com questões como a transferência internacional de dados, a jurisdição extraterritorial e a resolução de conflitos. Ele também destaca a necessidade de estabelecer padrões internacionais de proteção de dados, que possam ser adotados por diferentes jurisdições, a fim de promover a interoperabilidade e a harmonização regulatória (KUNER, 2021).

O autor ressalta que a eficácia da regulação transnacional da proteção de dados pessoais depende do fortalecimento dos mecanismos de "enforcement", incluindo a cooperação em investigações e a aplicação de sanções coordenadas.

Neste sentido, Christopher Kuner conclui que a abordagem dos desafios da regulação transnacional da proteção de dados pessoais requer um esforço conjunto e contínuo da comunidade internacional, visando garantir a proteção dos direitos fundamentais dos indivíduos na era digital (KUNER, 2021).

Nessa temática, é consabido que a Sociedade da Informação, impulsionada pelo avanço das tecnologias de informação e comunicação (TICs), trouxe consigo uma série de benefícios, como a facilidade de acesso à informação, a comunicação instantânea e a globalização dos mercados.

No entanto, esse mesmo ambiente digital também se tornou terreno fértil para a prática de crimes cibernéticos, que se aproveitam das vulnerabilidades e da sensação de anonimato proporcionada pela internet (PINHEIRO, 2021).

2. CRIMES CIBERNÉTICOS E LEGISLAÇÕES

Os crimes cibernéticos têm sido objeto de crescente atenção por parte da doutrina jurídica, em razão de suas peculiaridades e desafios para a prevenção e repressão. Nessa senda, Augusto Eduardo de Souza Rossini (2021) faz uma abrangente análise dos crimes informáticos, telemáticos e cibernéticos no contexto do Direito Penal e Processual Penal brasileiro. O autor discute a tipificação desses delitos, examinando as leis e normas existentes, bem como as lacunas e desafios na definição legal de condutas criminosas no ambiente digital.

Rossini também aborda as questões relacionadas à investigação desses crimes, destacando as peculiaridades e dificuldades na obtenção de provas eletrônicas, a necessidade de cooperação internacional e os limites impostos pelos direitos fundamentais dos investigados. Além disso, o autor analisa o processamento dos crimes informáticos, telemáticos e

cibernéticos, discutindo aspectos como competência jurisdicional, validade das provas digitais e aplicação de penas (ROSSINI, 2021).

Da mesma forma, Patrícia Peck Pinheiro (2021), em sua análise sobre os aspectos jurídicos da criminalidade digital, enfatiza a necessidade de uma abordagem multidisciplinar e da cooperação internacional para o efetivo combate a esses delitos. A autora destaca que a natureza transnacional e a complexidade técnica dos crimes digitais exigem a colaboração entre diferentes áreas do conhecimento, como o Direito, a tecnologia da informação e a segurança cibernética.

A autora também ressalta a importância da cooperação entre países, por meio de acordos internacionais e da atuação de organismos supranacionais, para a harmonização legislativa, o compartilhamento de informações e a realização de investigações conjuntas. A obra de Pinheiro contribui para a compreensão dos desafios jurídicos impostos pela criminalidade digital e aponta caminhos para o seu enfrentamento, a partir de uma perspectiva global e interdisciplinar.

Importante contribuição de Ana Elisa Liberatore Silva Bechara (2021). Sua análise sobre os desafios da responsabilidade penal na era digital discute questões fundamentais relacionadas à imputação objetiva, à autoria e à participação nos crimes cibernéticos. A autora aborda a dificuldade em se estabelecer o nexo causal entre a conduta do agente e o resultado danoso nos delitos praticados no ambiente virtual, bem como a complexidade na identificação dos autores e partícipes, dado o anonimato proporcionado pela internet.

Bechara também examina a aplicabilidade de teorias tradicionais da responsabilidade penal, como a teoria do domínio do fato, aos crimes cibernéticos, apontando a necessidade de adaptação e reinterpretação desses conceitos.

No âmbito internacional, a Convenção de Budapeste sobre o Cibercrime (EUROPE UNION, 2001) estabeleceu diretrizes para a harmonização das legislações nacionais e a cooperação internacional no combate a esses crimes, servindo como referência para diversos países. Autores como Marco Gercke (2021) e Ulrich Sieber (2021) analisam os desafios e as perspectivas do Direito Penal Internacional na prevenção e repressão da criminalidade cibernética.

Os crimes cibernéticos podem ser definidos como condutas ilícitas praticadas por meio de dispositivos eletrônicos e redes de computadores, visando à obtenção de vantagens indevidas

ou à causação de danos a terceiros (ROSSINI, 2021). Também podem ser classificados em diferentes categorias, de acordo com o bem jurídico violado e o modus operandi utilizado pelos criminosos.

Dentre as principais categorias, destacam-se (ROSSINI, 2021): (i) Crimes contra a confidencialidade, integridade e disponibilidade de sistemas e dados informáticos: acesso não autorizado a sistemas (*hacking*), interceptação ilegal de dados, interferência em sistemas e dados e uso indevido de dispositivos; (ii) Crimes relacionados ao conteúdo: pornografia infantil, discurso de ódio e discriminação, violação de direitos autorais (pirataria) e *fake news* e desinformação; (iii) Crimes relacionados à privacidade e à proteção de dados pessoais: violação de privacidade, roubo de identidade, vazamento de dados pessoais e espionagem cibernética; e (iv) Crimes financeiros e fraudes eletrônicas: *phishing* e golpes financeiros, fraudes em meios de pagamento eletrônico, lavagem de dinheiro digital e esquemas de pirâmide e investimentos fraudulentos.

A prática desses crimes é facilitada por diversos fatores, como a transnacionalidade das condutas, a dificuldade de rastreamento e identificação dos autores, a rapidez na disseminação de informações e a falta de conscientização dos usuários sobre os riscos do ambiente virtual (BARRETO; BRASIL, 2021). Além disso, a Sociedade da Informação também apresenta desafios específicos para a investigação e punição desses crimes.

A coleta de provas digitais, por exemplo, requer conhecimentos técnicos especializados e pode esbarrar em questões de jurisdição e cooperação internacional (PINHEIRO, 2021). A criptografia e o uso de redes anônimas, como a *deep web* e a *dark web*, também dificultam o trabalho das autoridades (LEONARDI, 2021).

Para enfrentar esses desafios, é necessário um constante aprimoramento da legislação, com a tipificação de novas condutas e a previsão de sanções adequadas à gravidade dos crimes cibernéticos.

2.1. Legislações Pertinentes

A Convenção de Budapeste sobre o Cibercrime, de 2001, foi um marco importante nesse sentido, estabelecendo diretrizes para a harmonização das legislações nacionais e a cooperação internacional no combate a esses crimes (EUROPE UNION, 2001). A Convenção de Budapeste sobre o Cibercrime, adotada em 2001 pelo Conselho da Europa, representou um marco significativo na luta contra os crimes cibernéticos. Essa convenção internacional

estabeleceu uma estrutura abrangente para lidar com uma variedade de crimes cometidos por meio de computadores e redes de comunicação, incluindo fraudes online, pornografia infantil, violações de direitos autorais, ataques cibernéticos e muitos outros.

Um dos principais objetivos da Convenção de Budapeste foi promover a harmonização das legislações nacionais relacionadas ao cibercrime, garantindo que os países signatários adotassem medidas adequadas para prevenir, investigar e punir esses tipos de crimes. Além disso, a convenção estabeleceu diretrizes para a cooperação internacional entre os Estados membros, visando facilitar o intercâmbio de informações, evidências e assistência legal em casos de cibercrime transnacional.

No Brasil, a Lei nº 12.737/2012, conhecida como "Lei Carolina Dieckmann", tipificou alguns crimes cibernéticos, como a invasão de dispositivos informáticos e a interrupção ou perturbação de serviços telegráficos, telefônicos, informáticos, telemáticos ou de informação de utilidade pública (Brasil, 2012). Mais recentemente, a Lei nº 13.709/2018, a Lei Geral de Proteção de Dados (LGPD), estabeleceu regras para o tratamento de dados pessoais e previu sanções para as violações a esses direitos (BRASIL, 2018).

A LGPD é uma legislação pioneira no Brasil, concebida a partir da influência do Regulamento Geral de Proteção de Dados (GDPR) da União Europeia. Seu desígnio primordial consiste em salvaguardar a privacidade e a integridade das informações pessoais dos indivíduos brasileiros. representa uma evolução significativa no panorama jurídico brasileiro, estabelecendo um conjunto abrangente de normas e diretrizes para o tratamento de dados pessoais. Inspirada no Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, a LGPD visa não apenas proteger a privacidade dos cidadãos, mas também promover uma cultura de responsabilidade e transparência no manejo de informações pessoais por parte das organizações.

Um dos pilares fundamentais da LGPD é o princípio da proteção de dados desde a concepção e por padrão, o que significa que a segurança e a privacidade devem ser consideradas desde a fase inicial do desenvolvimento de produtos e serviços, e integradas de forma intrínseca em todas as operações que envolvam o tratamento de dados pessoais. Além disso, esta lei estabelece uma série de direitos para os titulares dos dados, tais como o direito de acesso às informações que uma organização detém sobre eles, o direito de retificação de dados incorretos, o direito à portabilidade dos dados, entre outros. Esses direitos conferem aos indivíduos maior

controle sobre suas informações pessoais e garantem que eles possam exercer sua autodeterminação informativa de maneira eficaz.

No que diz respeito às organizações, a LGPD impõe uma série de obrigações, incluindo a realização de avaliações de impacto à privacidade, a implementação de medidas de segurança adequadas para proteger os dados pessoais e a notificação de incidentes de segurança que possam comprometer a proteção dessas informações.

Ademais, esta lei prevê sanções administrativas para as organizações que não cumprirem suas disposições, incluindo multas que podem chegar a até 2% do faturamento da empresa, limitadas a R$ 50 milhões por infração. Essas sanções têm o objetivo de garantir o cumprimento da lei e incentivar as organizações a adotarem práticas adequadas de proteção de dados.

Concorrentemente, o Marco Civil da Internet, formalmente conhecido como Lei nº 12.965/2014, é uma legislação brasileira que estabelece princípios, direitos e deveres para o uso da internet no país. Promulgado em abril de 2014, o Marco Civil representa uma referência importante para a governança da internet e para a proteção dos direitos dos usuários no ambiente digital.

Uma das características mais distintivas desta lei é a defesa da neutralidade da rede, princípio que garante que todos os dados trafeguem na internet de forma igualitária, sem discriminação ou priorização indevida por parte dos provedores de acesso. Isso significa que os provedores de internet não podem bloquear, priorizar ou interferir no tráfego de dados com base em interesses comerciais ou políticos.

Além da neutralidade da rede, o Marco Civil estabelece direitos fundamentais para os usuários da internet, como a proteção da privacidade e dos dados pessoais, a liberdade de expressão, a proteção da intimidade e da vida privada, entre outros. A legislação também define princípios de transparência, responsabilidade e prestação de contas para os provedores de internet e os usuários.

Outro aspecto relevante é a previsão de mecanismos de responsabilização dos provedores de internet em casos de violações de direitos dos usuários, como difamação, invasão de privacidade, violação de direitos autorais, entre outros.

O Marco Civil da Internet estabelece que os provedores de internet devem agir de forma diligente para remover conteúdos ilegais após uma ordem judicial específica, garantindo

ao mesmo tempo o direito à ampla defesa e ao contraditório. Além disso, prevê a proteção da privacidade dos usuários e o tratamento adequado de seus dados pessoais pelos provedores de internet, estabelecendo diretrizes claras para a coleta, o armazenamento, o uso e a divulgação de informações pessoais na internet.

No entanto, em que pese a farta previsão legal contra abusos cometidos no âmbito virtual, meios tão somente legais não são suficientes para o efetivo combate aos crimes cibernéticos. É necessário também investir em capacitação e treinamento das autoridades policiais e judiciárias, bem como em campanhas de conscientização da população sobre os riscos e as formas de prevenção desses crimes (PINHEIRO, 2021).

Outra medida importante é o estabelecimento de parcerias entre o poder público e o setor privado, especialmente com as empresas de tecnologia e provedores de serviços de internet. Essas parcerias podem viabilizar o desenvolvimento de soluções tecnológicas para a prevenção e detecção de crimes cibernéticos, bem como facilitar a cooperação na investigação e punição dessas condutas (LEONARDI, 2021).

Por fim, é fundamental que a sociedade como um todo esteja engajada no combate aos crimes cibernéticos. Isso inclui a adoção de boas práticas de segurança digital, como o uso de senhas fortes, a atualização regular de softwares e a desconfiança em relação a links e anexos suspeitos. Também é importante que os usuários estejam atentos aos seus direitos e saibam como proceder em caso de violações, buscando orientação junto às autoridades competentes (BARRETO; BRASIL, 2021).

Em suma, os crimes cibernéticos representam uma ameaça crescente na Sociedade da Informação, exigindo uma abordagem multidisciplinar e a colaboração entre todos os setores da sociedade para o seu efetivo enfrentamento. Somente com a combinação de medidas legislativas, tecnológicas, educativas e de cooperação internacional será possível construir um ambiente virtual mais seguro e justo para todos.

Percebe-se, nesse contexto, que a Sociedade da Informação, ao mesmo tempo em que proporciona inúmeros benefícios, como a facilidade de comunicação e acesso à informação, também cria um ambiente propício para a prática desses crimes. A sensação de anonimato e a facilidade de acesso a ferramentas tecnológicas contribuem para o aumento da criminalidade virtual (BARRETO; BRASIL, 2021).

2.2. Investigação e Desafios

Inicialmente, tem-se que, para investigar e punir os crimes cibernéticos, as autoridades muitas vezes precisam ter acesso a dados pessoais e informações sigilosas dos usuários, o que pode conflitar com o direito à privacidade (LEONARDI, 2021). A quebra de sigilo de dados e comunicações, quando necessária para a elucidação de crimes, deve ser realizada de forma proporcional e com autorização judicial, respeitando as garantias constitucionais dos investigados (BARRETO; BRASIL, 2021).

Ademais, muitos crimes cibernéticos, como o roubo de identidade e o vazamento de dados pessoais, estão diretamente relacionados à violação da privacidade dos usuários (PINHEIRO, 2021). As empresas que coletam e tratam dados pessoais devem adotar medidas de segurança adequadas para prevenir o acesso não autorizado e o uso indevido dessas informações, em conformidade com a legislação de proteção de dados, como a LGPD no Brasil e o GDPR na União Europeia (BRASIL, 2018; EUROPEAN UNION, 2016).

Outro ponto é que, no combate aos crimes cibernéticos, que muitas vezes têm caráter transnacional, requer a cooperação entre diferentes países e o compartilhamento de informações entre as autoridades competentes (ROSSINI, 2021). Essa cooperação deve ser realizada de forma a respeitar a soberania dos Estados e as garantias fundamentais dos indivíduos, encontrando um equilíbrio entre a eficácia das investigações e a proteção da privacidade dos envolvidos (LEONARDI, 2021).

Observa-se que a investigação de crimes cibernéticos suscita uma problemática singular, uma vez que demanda a abordagem de desafios específicos. Isso requer habilidades técnicas especializadas e a implementação de estratégias distintas quando comparada à investigação de crimes convencionais. Um dos principais aspectos relaciona-se às evidências digitais, como registros de acesso, logs de comunicação, arquivos e metadados, são fundamentais para a elucidação de crimes cibernéticos (PINHEIRO, 2021). Isso porque a coleta dessas evidências deve ser realizada de forma a preservar a sua integridade e a cadeia de custódia, evitando a contaminação ou a perda de dados relevantes (BARRETO; BRASIL, 2021). Além disso, a análise das evidências digitais requer o uso de ferramentas e técnicas específicas, como a computação forense, a recuperação de dados e a quebra de criptografia (ROSSINI, 2021).

Outro ponto relaciona-se à cooperação entre diferentes órgãos e instituições. Uma vez que a investigação de crimes cibernéticos muitas vezes envolve a atuação de diferentes órgãos

e instituições, como a polícia judiciária, o Ministério Público, os provedores de serviços de internet e as empresas de tecnologia (LEONARDI, 2021), vê-se que é necessário estabelecer mecanismos de cooperação e compartilhamento de informações entre esses atores, respeitando as suas competências legais e as garantias processuais dos investigados (PINHEIRO, 2021). Some-se a isso que a cooperação internacional também é fundamental, uma vez que os crimes cibernéticos frequentemente ultrapassam as fronteiras nacionais, exigindo a articulação entre as autoridades de diferentes países (ROSSINI, 2021).

Aponte-se, ainda, a necessidade de se capacitar e especializar os profissionais envolvidos. Isso porque a investigação de crimes cibernéticos requer profissionais capacitados e especializados, com conhecimentos técnicos em áreas como tecnologia da informação, segurança cibernética e computação forense (BARRETO; BRASIL, 2021). Daí, então, ser necessário investir na formação e no treinamento contínuo desses profissionais, para que estejam atualizados em relação às novas tecnologias e às técnicas utilizadas pelos criminosos (PINHEIRO, 2021). Também, há a necessidade de se criar unidades especializadas em crimes cibernéticos, tanto no âmbito policial quanto no Ministério Público e no Poder Judiciário, pode contribuir para a eficácia das investigações e a uniformização dos procedimentos (LEONARDI, 2021).

Por fim, imperioso se buscar o respeito aos direitos fundamentais e às garantias processuais. Tem-se, assim que a investigação de crimes cibernéticos deve ser realizada em conformidade com os princípios do Estado de Direito e as garantias processuais dos investigados, como o devido processo legal, a ampla defesa e o contraditório (BARRETO; BRASIL, 2021). No entanto, medidas invasivas, como a quebra de sigilo de dados e comunicações, devem ser utilizadas de forma excepcional e proporcional, sempre com autorização judicial e respeitando os limites legais (PINHEIRO, 2021). O ideal, nessa busca, é encontrar um equilíbrio entre a eficácia das investigações e a proteção dos direitos fundamentais, como a privacidade, a liberdade de expressão e a presunção de inocência (LEONARDI, 2021).

Dessa problemática, vê-se que, para enfrentar esses desafios, é fundamental que haja um constante aprimoramento das técnicas e estratégias de investigação, bem como a atualização da legislação processual penal para contemplar as especificidades dos crimes cibernéticos. A cooperação entre os diferentes atores envolvidos e a capacitação dos profissionais também são

medidas essenciais para o sucesso das investigações (ROSSINI, 2021). Além disso, é importante promover a conscientização da sociedade sobre a importância da prevenção e da denúncia de crimes cibernéticos, bem como sobre os riscos e as consequências dessas condutas. A participação ativa dos cidadãos, em conjunto com a atuação das autoridades competentes, é fundamental para o enfrentamento efetivo dessa forma de criminalidade (PINHEIRO, 2021).

3. PRIVACIDADE E PROTEÇÃO DE DADOS

O direito à privacidade e à proteção de dados pessoais tem ganhado crescente relevância na Sociedade da Informação, em razão da coleta, armazenamento e processamento massivo de informações pessoais por empresas e governos. Dessa análise, verifica-se um dos principais desafios enfrentados pela Sociedade da Informação é tentar encontrar um ponto de equilíbrio entre o direito à privacidade e o direito à informação.

Um dos principais desafios enfrentados pelo Direito na Sociedade da Informação é o equilíbrio entre o direito à privacidade e o direito à informação. De um lado, os usuários têm o direito de ter sua privacidade protegida, evitando a exposição indevida de seus dados pessoais e informações sensíveis. Por outro lado, as autoridades necessitam de acesso a determinadas informações para investigar e punir os crimes cibernéticos (LEONARDI, 2021).

Esse conflito tem gerado intensos debates e discussões em âmbito nacional e internacional. A União Europeia, por exemplo, aprovou em 2018 o Regulamento Geral sobre a Proteção de Dados (GDPR), que estabelece regras rígidas para o tratamento de dados pessoais e prevê sanções severas para as empresas que descumprirem essas normas (EUROPEAN UNION, 2018). No Brasil, a Lei Geral de Proteção de Dados (LGPD) entrou em vigor em 2020, seguindo princípios semelhantes aos do GDPR (BRASIL, 2018).

No entanto, a aplicação dessas normas nem sempre é simples, especialmente quando se trata de investigações criminais. Em muitos casos, as autoridades precisam solicitar a quebra de sigilo de dados junto às empresas de tecnologia, o que pode gerar conflitos e questionamentos sobre a legalidade e a proporcionalidade dessas medidas (LEONARDI, 2021).

Outra questão a ser abordada é o ponto nevrálgico entre a liberdade de expressão e ao problemática do anonimato na internet. Tais temas têm sido objeto de intensos debates na Sociedade da Informação, em razão de sua importância para a democracia e a inovação, mas também de seus potenciais riscos e abusos. Eduardo Andrés Bertoni (2021) analisa a liberdade

de expressão na era digital, discutindo seus fundamentos, limites e desafios à luz do Direito Internacional dos Direitos Humanos.

Juliano Maranhão (2021) aborda a questão do anonimato na internet, analisando seus fundamentos constitucionais e sua relação com a liberdade de expressão e a privacidade. Já Ronaldo Lemos (2021) discute os desafios da regulação da liberdade de expressão na internet, enfatizando a necessidade de equilíbrio entre a proteção dos direitos fundamentais e a prevenção de abusos.

No âmbito internacional, a Declaração Conjunta sobre Liberdade de Expressão e Internet (ONU et al., 2011) estabeleceu diretrizes para a proteção da liberdade de expressão no ambiente digital, reconhecendo o direito ao anonimato e à utilização de criptografia. Autores como Wolfgang Benedek e Matthias C. Kettemann (2021) analisam os desafios da governança da internet para a proteção dos direitos humanos, destacando a importância da liberdade de expressão e do acesso à informação.

A revisão da literatura apresentada demonstra a complexidade e a relevância dos temas abordados neste artigo, fornecendo as bases teóricas e conceituais para a análise dos crimes cibernéticos e do equilíbrio entre privacidade e informação na Sociedade da Informação. A partir desses fundamentos, serão discutidos os desafios e as perspectivas para o Direito nesse contexto, buscando contribuir para o aprimoramento das respostas jurídicas e políticas a essas questões.

Para enfrentar esses desafios, é fundamental que haja um constante diálogo e cooperação entre os diferentes atores envolvidos, como o poder público, as empresas de tecnologia, a sociedade civil e a academia. A busca pelo equilíbrio entre privacidade e informação deve pautar-se pelos princípios da legalidade, da proporcionalidade e da transparência, sempre tendo como objetivo a proteção dos direitos fundamentais dos indivíduos e a construção de um ambiente virtual mais seguro e democrático (LEONARDI, 2021).

Além disso, é necessário investir em educação e conscientização dos usuários sobre os seus direitos e deveres no ambiente digital, bem como sobre as medidas de segurança e prevenção de crimes cibernéticos. Somente com a participação ativa e informada de todos os setores da sociedade será possível encontrar soluções efetivas e equilibradas para os desafios impostos pela Sociedade da Informação (PINHEIRO, 2021).

3.1. Liberdade de expressão e anonimato na internet

A liberdade de expressão e o anonimato na internet são temas complexos e controversos, que envolvem a ponderação entre direitos fundamentais e a necessidade de prevenir e punir crimes cibernéticos.

Nesse contexto, tem-se que a liberdade de expressão é um direito fundamental, consagrado em tratados internacionais e constituições nacionais, que inclui a liberdade de manifestar opiniões, ideias e informações por qualquer meio, inclusive pela internet (LEONARDI, 2021). A internet ampliou significativamente as possibilidades de exercício da liberdade de expressão, permitindo que qualquer pessoa possa se manifestar e participar do debate público, sem as limitações dos meios de comunicação tradicionais (PINHEIRO, 2021). A liberdade de expressão é essencial para a democracia, o pluralismo e a inovação, devendo ser protegida e promovida no ambiente digital (BARRETO; BRASIL, 2021).

Ademais, a liberdade de expressão não é um direito absoluto, podendo ser limitada em casos excepcionais, quando necessário para proteger outros direitos fundamentais ou interesses legítimos (ROSSINI, 2021). Esses limites incluem a proibição de discursos de ódio, incitação à violência, violação da privacidade, difamação, entre outros (LEONARDI, 2021). A definição desses limites deve ser clara e precisa, evitando a censura prévia e o efeito inibidor sobre a liberdade de expressão. As restrições devem ser proporcionais e justificadas, submetidas ao controle judicial (PINHEIRO, 2021).

Nesse contexto, importante apontar que o anonimato e o pseudonimato são formas de exercício da liberdade de expressão na internet, permitindo que as pessoas se manifestem sem revelar sua identidade real (BARRETO; BRASIL, 2021). Essas formas de expressão podem ser importantes para proteger a privacidade, a segurança e a liberdade de grupos vulneráveis, como dissidentes políticos, minorias e denunciantes (LEONARDI, 2021). No entanto, o anonimato também pode ser utilizado para a prática de crimes cibernéticos, como a disseminação de discursos de ódio, fake news e violações da privacidade (ROSSINI, 2021).

Aponte-se, também, que o desafio é encontrar um equilíbrio entre a proteção da liberdade de expressão e o anonimato na internet e a necessidade de prevenir e punir crimes cibernéticos (PINHEIRO, 2021). Esse equilíbrio pode ser alcançado por meio de medidas como a moderação de conteúdo pelas plataformas, com base em termos de uso claros e transparentes, e a possibilidade de responsabilização dos autores de condutas ilícitas, mediante ordem judicial (LEONARDI, 2021). A educação e a conscientização dos usuários também são fundamentais

para promover um ambiente digital mais saudável e respeitoso, combatendo a desinformação e o discurso de ódio (BARRETO; BRASIL, 2021).

Para enfrentar esses desafios, é necessário um diálogo constante entre os diferentes atores envolvidos, como governos, empresas, sociedade civil e academia. A regulação da internet deve ser equilibrada e proporcional, evitando medidas excessivas que possam comprometer a liberdade de expressão e a inovação (ROSSINI, 2021).

Além disso, é importante investir em pesquisas e desenvolvimento de tecnologias que possam conciliar a proteção da liberdade de expressão e do anonimato com a prevenção e o combate a crimes cibernéticos, como a criptografia, a análise de dados e a inteligência artificial (PINHEIRO, 2021).

3.2. Coleta e tratamento de dados pessoais

A coleta e o tratamento de dados pessoais têm se tornado cada vez mais relevantes na Sociedade da Informação, especialmente no contexto dos crimes cibernéticos. O uso indevido dessas informações pode levar a graves violações da privacidade dos indivíduos e facilitar a prática de condutas ilícitas.

Assim, a coleta de dados pessoais deve ser realizada de forma transparente, informando claramente aos titulares sobre a finalidade, a forma e a extensão do tratamento (PINHEIRO, 2021). O consentimento do titular é um requisito essencial para a coleta e o tratamento de dados pessoais, devendo ser livre, informado e específico para cada finalidade (BRASIL, 2018; EUROPEAN UNION, 2016). As exceções ao consentimento, como o tratamento de dados para o cumprimento de obrigações legais ou para a proteção de interesses vitais do titular, devem ser interpretadas de forma restritiva e proporcional (LEONARDI, 2021).

O tratamento de dados pessoais deve observar os princípios da finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança e prevenção, não discriminação e responsabilização (Brasil, 2018; European Union, 2016). Esses princípios visam garantir que o tratamento de dados seja realizado de forma legítima, proporcional e segura, respeitando os direitos dos titulares e evitando abusos ou desvios de finalidade (PINHEIRO, 2021).

As empresas e organizações que realizam o tratamento de dados pessoais devem adotar medidas técnicas e administrativas adequadas para garantir a segurança dessas informações e prevenir incidentes como vazamentos, acessos não autorizados e alterações

indevidas (ROSSINI, 2021). Essas medidas incluem a criptografia de dados, o controle de acesso, a realização de auditorias e testes de segurança, a capacitação dos funcionários e a elaboração de planos de resposta a incidentes (LEONARDI, 2021). Em caso de incidentes de segurança que possam acarretar riscos ou danos aos titulares, as empresas devem comunicar imediatamente a autoridade nacional de proteção de dados e, quando necessário, os próprios titulares afetados (BRASIL, 2018; EUROPEAN UNION, 2016).

As empresas e organizações que realizam o tratamento de dados pessoais devem ser responsabilizadas por eventuais violações à legislação de proteção de dados e aos direitos dos titulares (PINHEIRO, 2021). A legislação prevê sanções administrativas, como advertências, multas e proibição parcial ou total do tratamento de dados, bem como a possibilidade de responsabilização civil e penal dos agentes envolvidos (BRASIL, 2018; EUROPEAN UNION, 2016). A aplicação efetiva dessas sanções é fundamental para coibir abusos e garantir a observância das normas de proteção de dados, contribuindo para a prevenção de crimes cibernéticos relacionados à violação da privacidade (LEONARDI, 2021).

Para enfrentar os desafios relacionados à coleta e ao tratamento de dados pessoais, é necessário um esforço conjunto entre o poder público, as empresas e a sociedade civil. A conscientização dos usuários sobre os seus direitos e a importância da proteção de seus dados é fundamental para a prevenção de abusos e a denúncia de violações (BARRETO; BRASIL, 2021).

Além disso, é essencial que haja uma fiscalização efetiva por parte das autoridades competentes, como a Autoridade Nacional de Proteção de Dados (ANPD) no Brasil, para garantir o cumprimento da legislação e a aplicação de sanções quando necessário. A cooperação internacional também é importante para lidar com o caráter transnacional do tratamento de dados e dos crimes cibernéticos a ele relacionados (ROSSINI, 2021).

Por fim, o desenvolvimento de tecnologias e soluções que promovam a proteção da privacidade desde a concepção (*privacy by design*) e a realização de avaliações de impacto à proteção de dados podem contribuir para a mitigação dos riscos e a promoção de boas práticas no tratamento de informações pessoais (PINHEIRO, 2021).

3.3. Cooperação Internacional e Compartilhamento de Informações

A cooperação internacional e o compartilhamento de informações são elementos essenciais para o enfrentamento dos crimes cibernéticos, uma vez que essas condutas

frequentemente ultrapassam as fronteiras nacionais e envolvem a atuação de criminosos em diferentes países.

Aspecto importante a ser apontado é que a celebração de tratados e acordos internacionais é fundamental para estabelecer as bases jurídicas da cooperação entre os países no combate aos crimes cibernéticos (ROSSINI, 2021). A Convenção de Budapeste sobre o Cibercrime, de 2001, é o principal instrumento internacional nessa área, prevendo medidas de harmonização das legislações nacionais, cooperação internacional e assistência mútua em matéria penal (EUROPE UNION, 2001). Outros acordos regionais e bilaterais também podem ser celebrados para aprofundar a cooperação e atender às especificidades de cada contexto (LEONARDI, 2021).

Aponte-se, ainda, que a assistência mútua em matéria penal é um dos principais mecanismos de cooperação internacional no combate aos crimes cibernéticos, permitindo a troca de informações e a realização de diligências entre as autoridades competentes de diferentes países (PINHEIRO, 2021). Essa assistência pode incluir a preservação e o fornecimento de dados eletrônicos, a coleta de evidências digitais, a tomada de depoimentos por videoconferência, a quebra de sigilo de dados e comunicações, entre outras medidas (BARRETO; BRASIL, 2021). Para que a assistência mútua seja efetiva, é necessário que os países adotem procedimentos ágeis e desburocratizados, respeitando as garantias processuais e os direitos fundamentais dos envolvidos (ROSSINI, 2021).

Outro aspecto é que a criação de redes de cooperação e pontos de contato entre as autoridades competentes de diferentes países é essencial para facilitar a troca de informações e a coordenação das investigações (LEONARDI, 2021). Essas redes podem ser estabelecidas no âmbito de organizações internacionais, como a Interpol e a Europol, ou por meio de iniciativas regionais e bilaterais (PINHEIRO, 2021). Os pontos de contato devem ser designados em cada país, preferencialmente no âmbito das unidades especializadas em crimes cibernéticos, para centralizar as demandas de cooperação e agilizar os procedimentos (BARRETO; BRASIL, 2021).

Nesse contexto, o compartilhamento de boas práticas e a capacitação conjunta dos profissionais envolvidos no combate aos crimes cibernéticos são medidas importantes para aprimorar a cooperação internacional (ROSSINI, 2021). A realização de workshops, seminários e treinamentos internacionais permite a troca de experiências, a atualização sobre

novas técnicas e tecnologias e a harmonização dos procedimentos entre os países (LEONARDI, 2021). A criação de plataformas online e bancos de dados compartilhados também pode facilitar o acesso a informações relevantes e a coordenação das ações de prevenção e repressão aos crimes cibernéticos (PINHEIRO, 2021).

Para que a cooperação internacional e o compartilhamento de informações sejam efetivos, é necessário superar alguns desafios, como as diferenças entre as legislações nacionais, as barreiras linguísticas e culturais, e a necessidade de garantir a segurança e a confidencialidade das informações trocadas (BARRETO; BRASIL, 2021).

Além disso, é fundamental que haja um equilíbrio entre a eficácia das medidas de cooperação e o respeito aos direitos fundamentais, como a privacidade, o devido processo legal e a soberania dos Estados. A atuação das autoridades deve pautar-se pelos princípios da legalidade, da proporcionalidade e da transparência, evitando abusos e garantindo a legitimidade das ações de combate aos crimes cibernéticos (LEONARDI, 2021).

Ainda, a cooperação internacional deve ser complementada por medidas de prevenção e conscientização da sociedade, envolvendo a participação de empresas, organizações da sociedade civil e instituições de ensino e pesquisa. Somente com um esforço conjunto e coordenado será possível enfrentar de forma efetiva a complexidade e a transnacionalidade dos crimes cibernéticos na Sociedade da Informação (PINHEIRO, 2021).

Por fim, a cooperação internacional também é essencial para lidar com a natureza transnacional da internet e dos crimes cibernéticos, buscando soluções harmonizadas e respeitando as especificidades de cada país. Somente com um esforço conjunto e multissetorial será possível construir uma internet mais livre, segura e democrática para todos (LEONARDI, 2021).

CONCLUSÃO

Para enfrentar os desafios impostos pelos crimes cibernéticos na Sociedade da Informação, é necessário um esforço conjunto entre o Direito, a tecnologia e a sociedade. Algumas possíveis soluções incluem: aprimoramento da legislação específica sobre crimes cibernéticos, com a tipificação de novas condutas e a previsão de sanções adequadas (ROSSINI, 2021), investimento em capacitação e treinamento das autoridades policiais e judiciárias para lidar com as especificidades dos crimes virtuais (PINHEIRO, 2021), cooperação internacional

para a investigação e punição de crimes transnacionais, por meio de acordos e tratados entre os países (BARRETO; BRASIL, 2021), conscientização da sociedade sobre os riscos e as formas de prevenção dos crimes cibernéticos, por meio de campanhas educativas e orientações de segurança (LEONARDI, 2021).

Além disso, é fundamental que haja um constante diálogo e equilíbrio entre o direito à privacidade e o direito à informação, buscando soluções que atendam aos interesses legítimos de todas as partes envolvidas. O direito à liberdade de expressão e ao anonimato na internet são pilares essenciais para o exercício pleno da cidadania e para fomentar o debate democrático. No entanto, é inegável que tais direitos também podem ser instrumentalizados para perpetrar crimes cibernéticos, incluindo a propagação de discursos de ódio e de desinformação (BARRETO; BRASIL, 2021). Diante desse cenário, torna-se imperativo efetivos meios para mitigar tais abusos no âmbito virtual, ainda que sejam evidenciados em medidas como a moderação de conteúdo e a responsabilização dos autores de condutas ilícitas são essenciais, sempre respeitando os princípios do devido processo legal e da proporcionalidade das sanções (PINHEIRO, 2021).

Diante da intrincada tessitura de desafios apresentados pelos delitos cibernéticos na contemporaneidade, é inescusável reconhecer que soluções verdadeiramente eficazes demandam uma abordagem multidisciplinar e sinérgica. Torna-se imprescindível que as estratégias delineadas para abordar essas questões não apenas abranjam as esferas jurídicas e tecnológicas, mas também incorporem as complexidades sociais e éticas subjacentes ao problema. Sob tal perspectiva, o aprimoramento normativo, o reforço da preparação das autoridades competentes, a promoção da cooperação internacional e a educação da sociedade acerca dos riscos e das medidas preventivas emergem como pilares inalienáveis na jornada rumo a um ambiente digital mais seguro e ético. A consecução de um equilíbrio equitativo entre a salvaguarda da privacidade e a preservação da liberdade de expressão constitui, ademais, um imperativo central a ser alcançado. Unicamente por intermédio de uma abordagem abrangente e colaborativa será possível mitigar os efeitos nefastos dos crimes cibernéticos e edificar uma sociedade digital mais resiliente e equitativa para todos os seus membros.

REFERÊNCIAS

BARRETO, Alessandro Gonçalves; BRASIL, Beatriz Silveira. Desafios do direito penal na sociedade da informação: uma análise dos crimes cibernéticos. **Revista Brasileira de**

Ciências Criminais, v. 175, p. 89-115, 2021.

BECHARA, Ana Elisa Liberatore Silva. O sentido da pena e a racionalidade de sua aplicação no estado democrático de direito brasileiro. *In*: **Os desafios das ciências criminais na atualidade**. Belo Horizonte: D'Plácido, 2021.

BENEDEK, Wolfgang Benedek; KETTEMANN, Matthias C. **Research Handbook on Human Rights and Digital Technology: Global Politics, Law and International Relations.** Cheltenham, UK: Edward Elgar Publishing, 2021.

BENKLER, Yochai. **The wealth of networks: how social production transforms markets and freedom.** New Haven: Yale University Press, 2021. Disponível em: https://benkler.org/Benkler_Wealth_Of_Networks.pdf. Acesso em: 28 out. 2024.

BERTONI, Eduardo Andrés. **Libertad de expresión en la era digital**. Buenos Aires: CELE, 2021.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos. **Lei Carolina Dieckmann.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 30 mai. 2024.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 30 mai. 2024.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Marco Civil da Internet**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 09 dez. 2024.

CASTELLS, Manuel. **A Sociedade em Rede**. 8. ed. São Paulo: Paz e Terra, 2018. v. 1. Disponível em: https://drive.google.com/file/d/0B2vyKSOtK2MkMjdiZTYxZWMtYmMyMy00MjBlLThjYmYtNTBmZDBkZjRiMTYy/view?hl=pt-BR&pli=1&resourcekey=0-OL6vup9M3JUjPHAbvCTD5Q. Acesso em: 28 out. 2024.

DE HERT, Paul; GUTWIRTH, Serge. Data protection in the case law of Strasbourg and Luxembourg: constitutionalization in action. *In*: GUTWIRTH, Serge; POULLET, Yves; DE HERT, Paul; DE TERWANGNE, Cécile; NOUWT, Sjaak (eds.) **Reinventing data protection?** Dordrecht: Springer, 2021. p. 3-44.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados.** 3. ed. São Paulo: Thomson Reuters Brasil, 2021.

EUROPEAN UNION (UE). **Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the**

processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj. Acesso em: 30.mai.2024.

GERCKE, Marco. International criminal law in cyberspace: challenges and perspectives. *In*: HAUCK, Pierre; PETERKE, Sven (eds.). **International law and transnational organised crime**. Oxford: Oxford University Press, 2021. p. 167-189.

FREEMAN, Christopher, SOETE, Luc. **The Economics of Industrial Innovation**. 2 ed. London (UK): Francis Pinter, 1982.

KUNER, Christopher. **Transborder data flows and data privacy law.** 2. ed. Oxford: Oxford University Press, 2021.

LEMOS, Ronaldo. **Liberdade de expressão, remoção de conteúdo e direito ao esquecimento na internet.** *In*: SCHREIBER, Anderson (coord.). Direito e mídia. São Paulo: Atlas, 2021. p. 347-367.

LEONARDI, Marcel. **Tutela e privacidade na internet.** 2. ed. São Paulo: Saraiva, 2021.

LÉVY, Pierre. **Cibercultura.** 3. ed. São Paulo: Editora 34, 2021. Disponível em: https://drive.google.com/file/d/0ByGOj9_gW1Y7QnFhVEhKVzZpUXc/view?resourcekey=0-wCXbiCtmOTKZx1hd-55lQQ . Acesso: 28 out. 2024.

MARANHÃO, Juliano. Anonimato e liberdade de expressão na internet. *In*: PINHEIRO, Patrícia Peck. (coord.). **Direito digital aplicado 4.0**. 2. ed. São Paulo: Thomson Reuters Brasil, 2021. p. 197-212.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014. Disponível em: http://bdjur.stj.jus.br/dspace/handle/2011/76233. Acesso em: 28 out. 2024.

PINHEIRO, Patrícia Peck. **Direito digital**. 7. ed. São Paulo: Saraiva, 2021.

RODOTÀ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje**. Rio de Janeiro: Renovar, 2021.

ROSSINI, Augusto Eduardo de Souza. **Informática, telemática e direito penal.** 2. ed. São Paulo: Almedina, 2021.

SIEBER, Ulrich. Cybercrime and jurisdiction in the global information society. *In*: SIEBER, U.; BRUNST, Philip W. (eds.). **Cyberterrorism and cybercrime: vulnerabilities and international responses**. Freiburg: Max Planck Institute for Foreign and International Criminal Law, 2021.

7 Information Society and Law
FMU CENTRO UNIVERSITÁRIO

A REGULARIZAÇÃO JURÍDICA BRASILEIRA VOLTADA À UTILIZAÇÃO DE ROBÔS

BRAZILIAN LEGAL REGULARIZATION AIMING AT THE USE OF ROBOTS

Ronny Max Machado[1]; João Francisco Mantovanelli[2]

Resumo: O presente resumo expandido tem por objetivo apontar a importância da criação de um marco regulatório dos robôs no Brasil, considerando a sua relevância no ambiente da sociedade brasileira.
Palavras-chave: Robôs; Tecnologia; Regulação.

Abstract: This expanded summary aims to highlight the importance of creating a regulatory framework for robots in Brazil, considering their relevance in the Brazilian society environment.
Keywords: Robots; Technology; Regulation.

INTRODUÇÃO

É importante destacar que com o passar dos anos a sociedade estava acostumada e acomodada com o estilo de vida agrário e campestre e no campo de trabalho era mais voltado ao costume artesanal. Com os anos surgiu a globalização e desta forma nasceu a modernidade advindo de outras culturas incorporadas à sociedade brasileira. O presente resumo expandido, por meio da metodologia da revisão bibliográfica, tem por finalidade apontar a importância da criação de um marco regulatório dos robôs no Brasil, considerando a sua relevância no ambiente da sociedade brasileira.

DISCUSSÕES E RESULTADOS

A expressão “globalização” também comporta outras nomenclaturas, de acordo com a

[1] Mestre em Direito da Sociedade da Informação pelo Centro Universitário das Faculdades Metropolitanas Unidas. São Paulo. Estado de São Paulo. Brasil. Pesquisador junto ao Programa de Mestrado em Direito da Sociedade da Informação pelo Centro Universitário das Faculdades Metropolitanas Unidas. São Paulo. Estado de São Paulo. Brasil

[2] Graduado em Direito pela Faculdade de Americana -FAM (2009-2013). Pós-graduado em Direito Urbanístico e Meio Ambiente pela Damásio Educacional (2021-2022). Pesquisador junto ao Programa de Mestrado em Direito da Sociedade da Informação pelo Centro Universitário das Faculdades Metropolitanas Unidas. São Paulo. Estado de São Paulo. Brasil.

explicação de Nanci de Melo e Silva:

> A globalização ou mundialização (a primeira no sentido anglo-saxão e a segunda no entendimento francês) possui vários significados, que traduzem um fenômeno econômico como consequência do liberalismo que emerge de um mercado comum interdependente. Tida, por alguns, como fenômeno ideológico, a globalização, etapa mais recente da história das relações entre os homens e suas organizações, apresenta as seguintes fases: Bilateralismo; Multilateralismo; Transnacionalismo. O direito moderno, principal meio ou instrumento de regulação estatal, tem sofrido profundas alterações. A consequência é a evolução da técnica jurídica, com maior flexibilidade do caráter autoritário do direito. O direito nacional aproxima-se do direito internacional, na fase de integração dos dias atuais. Surge um direito procedente de negociações, constituindo uma tentativa para encontrar uma nova forma de regulamentação, cabendo ao direito redefinir as novas tendências (Silva, 2002).

Nos maquinários eletrônicos e a utilização de computadores, assim como na vida cotidiana das famílias, os eletrodomésticos digitais e o surgimento de relógios de pulsos que eram analógicos substituindo para relógios digitais surgiram, bem como, os automóveis advindos de um processo industrial cada vez mais avançado, servem de ilustração para que o progresso tecnológico que viria. Com o advento da globalização e abertura de livre comércio internacional ocasionou à necessidade de mão de obra laboral com capacidade técnica em manipular maquinários eletrônicos desde a linha de montagem até a automação e programação. O mercado de trabalho ficou muito mais seletivo, principalmente em regiões agrárias brasileira, onde trabalhadores foram substituídos por máquinas como, por exemplo, as colheitadeiras, usadas em lavouras de soja, café e de cana-de-açúcar, havendo desemprego e o êxodo rural. Em indústrias automobilísticas, têxteis e alimentícias, houve a substituição de máquinas artesanais como chave de rodas, por parafusadeiras elétricas, teares eletrônicos e esteiras autônomas, bem como as máquinas cortadeiras e empacotadeiras que não exigem mais funcionários que antes faziam esses processos de forma braçal. Havendo demissões em massa, em determinas empresas houve a formação técnica e administrativa para que as equipes foram ambientadas em manusearem estas máquinas com treinamentos regulares e atuarem dentro de normas regulares, para estarem em conformidade com o controle de qualidade. Nesta sociedade pós-moderna com esse avanço dinâmico dentro do mercantilismo nas sociedades agrária e urbana desencadeia a invencibilidade em produções científicas, maquinárias e de tecnologia, devido à social evolução moderna. Luc Ferry (2015, p. 23) explica que:

> Logo, desemprego, desigualdade, mas também, durante os primeiros passos, decrescimentos: sem falar, como acabou de fazer, nos vendedores de discos que desapareceram, ou dos livreiros que hoje são ameaçados pelos tablets e pelas vendas on-line, é preciso ver que antes de produzir efeitos positivos em termos de consumo e de emprego, a revolução digital supunha que se investisse com risco. (FERRY, 2015, p. 23).

E com a sociedade industrial cada vez mais em ebulição surge a nanotecnologia, bem como a biotecnologia e desta maneira implica na área jurídica em reformulações de questões legislativas frente à utilização de robôs, levando-se em consideração às searas ambiental, social e trabalhista justamente por englobar direitos coletivos e difusos por construir e gerar proteção à sociedade civil e aos acessos ambientais, vide de modo taxativo e exegético, ao artigo 1 inciso III da Constituição Federal: Dignidade da Pessoa Humana. Para fins metodológico, conceitua-se os robôs como sendo:

> um objeto artificial que se parece com um ser humano; [ou] máquinas que exercem certas funções especiais. Um robô é uma máquina computadorizada capaz de realizar tarefas complexas demais para qualquer cérebro vivo, a ser o do homem, e de um tipo que nenhuma máquina não-computadorizada, é capaz de executar. Em outras palavras, os robôs podem ser definidos através da equação: robô= máquina + computador (Asimov, 1994, p.11).

Em outros dizeres:

> Na prática, um robô é um dispositivo autônomo ou semiautônomo que realiza trabalhos de acordo com um controle humano, controle parcial com supervisão, ou de forma autônoma. Além de serem usados como redutor de custos pela indústria, entende-se que a grande vocação para os robôs fica por conta da realização de tarefas em locais inóspitos ou impróprios a presença do ser humano. (Reis; Souza, 2020).

Isto posto, serve de bojo para a regularização fundamental diante dos impactos de se evitar e/ ou assegurar responsabilidades frente dos prejuízos que possam causar os robôs. Como por exemplo, ao meio ambiente através de drones nas lavouras por atuar sobre sistemas ecológicos. E no âmbito de saúde pública ou privada robôs que exercem procedimentos de aspecto semiautônomo. Os instrumentos legais visam à qualidade de vida desde os recursos ambientais e humanos com as articulações que transformam sobre os processos cultural, econômico. Jurídico, político, social e trabalhista, por consolidar às concepções que abarcam à Dignidade Da Pessoa Humana, por dentro deste tecnológico progresso. Frisa-se que os direitos se interligam com as questões de bioengenharia e de biotecnologia por estabelecerem reflexões sobre os limites dentro dos limites do panorama jurídico aos avanços tecnológicos nos ditames desta sociedade pós-moderna. Enfatizando direitos humanos de quarta-geração.

No Brasil com a criação de tecnologias voltadas às indústrias e comércios sobretudo em linhas de produção, informação tecnológica, automação, tecnologia industrial e performance digital, com o foco em robôs. O código civil demonstra em seu artigo 186 a pureza em ação de responsabilizar às empresas que ao criarem e a implantarem robôs e que venham a lesar ao meio

ambiente e à saúde individual e coletiva destaca-se: “Aquele que por ação ou omissão voluntária. Negligência ou imprudência, violar direitos e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito”. Surgindo ao dever obrigacional de reparação de danos. A transformação de responsabilidade civil sempre será produzida por convergências de forças cujas tendências que por sua vez se originam da interrelação de acontecimentos em relações juntamente com os fenômenos sociais. Não se pode refletir em um único caminho com uma visão de sistema ambiental de desenvolvimento ecológico, econômico e social. A influência das circunstâncias cotidianas e laborais impactam a vida humana por ser uma relação moldada entre ciência e a justiça. Surge-se a responsabilidade civil pelos Produtos elaborados; Prejuízos ao consumidor de produtos e serviços tecnológicos e de informáticas; Prejuízos nucleares; Prejuízos ecológicos com impacto ao ambiente; Prejuízos advindos de biotecnologia e Prejuízos para a saúde humana. Isto posto, todos estes prejuízos elencados revelam à urgente necessidade de legislações que se adequem e responsabilizem às empresas. Comércios de cada prejuízo em razão dos malefícios que os robôs venham a causar e que possam tornarem-se agravantes diante da falta de moralidade jurídica frente à falta de licenciamentos ambientais e de regulação jurídica, juntamente com a ausência de agências reguladoras. Silvio de Salvo Venosa (2019, p. 301) aduz:

> Há um conceito de mercado internacional, representado por empresas mais poderosas que os próprios Estados. Essas empresas supranacionais ditam muitos dos costumes e das condutas particulares. Esses megagrupos influenciam e criam costumes e condutas sociais, difundidos que são pela facilidade das comunicações. Os mercados são atualmente globalizados. A bebida que é consumida aqui também é do outro lado do mundo; assim como as roupas, os automóveis, os alimentos etc. Os ordenamentos não podem ignorar e deixar de refletir proteção social contra os desmandos dessas pessoas jurídicas. (Venosa, 2019, p. 301).

CONCLUSÃO

Conclui-se que no campo jurídico por meio de seus códigos: Ambiental, Civil. Consumidor, Penal. Trabalhista sobre o prisma de Constituição Federal, com as jurisprudências, conseguem atingir a regulação dos fatos correlacionados que atingem as finalidades destas tecnologias pós modernistas, acompanhando sempre aos progressos de nanorrobôs, em parceria com as biotecnologias. Ademais, o principal marco regulatório no Brasil que afeta o uso de Inteligência Artificial é a Lei Geral de Proteção de Dados (LGPD) que consiste em uma legislação voltada a estabelecer diretrizes, muito rigorosas, sobre como deve se tratar os

registros pessoais, bem como a sua coleta, armazenamento e processamento de informações. Contudo, esta norma, ainda não avança sobre o tema dos robôs no Brasil.

Há uma nota técnica (NT 31) que foi anexada à NR 12 e, que, normatizou o uso dos robôs colaborativos no Brasil (RtIforma,2018). No entanto, em nomes das inúmeras vantagens dos robôs, entre as quais: O investimento em cobots é baixo se comparado aos robôs industriais, o que contribui muito para economia, bem como sua fácil programação (Loureiro,2018); no campo da eficiência, os cobots podem maximizar a produtividade da linha de produção. Os cobots tem uma funcionalidade versátil, podendo ser empregadas em diversos setores, entre as quais, tem-se a fabricação, embalagem, usinagem, moldagem, testes e inspeções (Curty; Marchi,2019); por fim, destaca-se a segurança e flexibilidade com que os cobots atuam. O princípio ético no sentido de vida sadia em coletividade em convivência é dotado de responsabilidades articuladas com a previsibilidade e a prudência mediante às questões conflituosas e delitivas para o fortalecimento de direitos humanos fundamentais, dentro desta ótica tecnológica e nanotecnologia pós contemporânea.

REFERÊNCIAS

ABDI. **Agenda brasileira para a Indústria 4.0.** Disponível em: <http://www.indus--tria40.gov.br/>. Acesso em: 20/10/2024

ASIMOV, Isaac. **Visões de robô.** Trad. Ronaldo Sergio de Biasi. Rio de Janeiro: Record, 1994, p. 11.

BRASIL. **Lei 13.709 de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da República Federativa do Brasil, 15 agosto de 2018. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 20/10/2024

CASTRO JÚNIOR, Marco Aurélio de. **Direito robótico?** Jornal Correio da Bahia, Salvador, 29 dez. 2000.

CURTY, Clara Martins; MARCHI, Guilherme Hebling de. **Desenvolvimento de um robô colaborativo de baixo custo aplicado à indústria** 4.0. 2019. Disponível em: https://dspace.mackenzie.br/items/d8188cdd-b25e-44af-9831-326c8eef340f Acesso em: 27/10/2024

DOS REIS, N. R. S., & DE SOUZA, L. H. R. **Robótica no Brasil**: relatos de pesquisa e desenvolvimento. 2020 Disponível em:

https://www.17snhct.sbhc.org.br/resources/anais/11/snhct2020/1599878133_ARQUIVO_249261821280538eb5ef8357d4079f68.pdf Acesso em 20/10/2024

FERY, Luc. A inovação destruidora: **Ensaio sobre a lógica das sociedades modernas**. Rio de Janeiro: Objetiva, 2015.

LOUREIRO, Cristiana Jesus. Cobots Na Indústria 4.0 Impactos Sociais e Económicos. 2018. Master's Thesis. Universidade da Beira Interior (Portugal). Disponivel em: https://ubibliorum.ubi.pt/bitstream/10400.6/9687/1/6514_13891.pdf Acesso em 20/10/2024

POLLUX. **Robô Colaborativo.** Disponível em: <https://www.pollux.com.br/solucoes/robotica- colaborativa/>. Acesso em: 20/10/2024

RT INFORMA. Nota Técnica do Ministério do Trabalho esclarece o uso de "Robôs Colaborativos" frente à NR 12. **Informativo da Confederação Nacional da Indústria** Ano 4 – Número 21 – outubro de 2018 – www.cni.com.brDisponível em: https://conexaotrabalho.portaldaindustria.com.br/media/publication/files/RT%20Informa%20N.%2021%20outubro%20-%20Nota%20Tecnica%20do%20Ministerio%20do%20Trabalho%20esclarece%20o%20uso%20de%20Robos%20Colaborativos%20frente%20a%20NR%2012.pdf Acesso em 20/10/2024

SILVA, Nanci de Melo e. **Da jurisdição constitucional.** Belo Horizonte: Del Rey, 2002.

VENOSA, Silvio de Salvo. **Introdução ao estudo de direito**. São Paulo: Atlas, 2019.

UNIVERSAL ROBOTS. **Nossa História.** Disponível em: <https://www.universal-robots.com/pt/sobre-a-universal-robots/nossa-historia/>. Acesso em: 20/10/2024.

7 Information Society and Law
FMU CENTRO UNIVERSITÁRIO

EQUIPAMENTOS INTELIGENTES: IMPACTOS DA IOT NA VIDA COTIDIANA, PRIVACIDADE E SEGURANÇA

SMART EQUIPMENT: IOT IMPACTS ON EVERYDAY LIFE, PRIVACY AND SECURITY

Ronny Max Machado[1]; Francisco Céu Pereira [2]

Resumo: Este resumo expandido, por meio da metodologia de revisão bibliográfica e indicação e análise de alguns dados estatísticos ilustrativos, tem por objetivo explorar a influência crescente dos equipamentos inteligentes em vários aspectos da vida cotidiana, com especial atenção às implicações para privacidade e segurança cibernética.
Palavras-chave: Equipamentos Inteligentes; Privacidade; Segurança.

Abstract: This expanded summary, through the methodology of bibliographic review and indication and analysis of some illustrative statistical data, aims to explore the growing influence of smart equipment in various aspects of everyday life, with special attention to the implications for privacy and cybersecurity.
Keywords: Smart Equipment; Privacy; Security.

INTRODUÇÃO

O mundo globalizado trouxe a sociedade da informação (ou sociedade da comunicação), que difere da sociedade de conhecimento porque é uma expressão utilizada pela Unesco, que traduz a implantação de um conhecimento informacional. No Mundo, temos uma sobrecarga de informação de se divide em útil e inútil. A informação só passa a ser conhecimento quando ela ingressa no intelecto humano. Este resumo expandido, através da metodologia de revisão bibliográfica e indicação e análise de alguns dados estatísticos ilustrativos, tem por finalidade explorar a crescente influência dos equipamentos inteligentes em inúmeros aspectos da vida cotidiana, com especial atenção às implicações para privacidade e segurança cibernética.

[1] Mestre em Direito da Sociedade da Informação pelo Centro Universitário das Faculdades Metropolitanas Unidas. São Paulo. Estado de São Paulo. Brasil. Pesquisador junto ao Programa de Mestrado em Direito da Sociedade da Informação pelo Centro Universitário das Faculdades Metropolitanas Unidas. São Paulo. Estado de São Paulo. Brasil

[2] Cursando o sétimo o 9º semestre de Direito da Faculdade Dom Adélio Tomasin (FADAT) Quixadá, Ceará, Brasil; Pesquisador junto ao Programa de Mestrado em Direito da Sociedade da Informação pelo Centro Universitário das Faculdades Metropolitanas Unidas, São Paulo; Pesquisador junto ao Grupo de Pesquisa DigiCult vinculado a Graduação e Mestrado em Direito da UFERSA, Rio Grande do Norte.

DISCUSSÕES E RESULTADOS

A denominada revolução informacional produziu uma série de efeitos, entre os quais, o fenômeno de transnacionalização e o advento dos blocos econômicos, o surgimento do *e-commerce*, a ideia de economicidade, a elaboração de um banco de dados, bem como a circulação de dados por meios eletrônicos e disposição de normas de caráter comunitário. Nos dizeres de Machado, Barreto e Peccicacco é a importância da informação na contemporaneidade, de maneira que:

> pode-se apontar que uma grande parcela da população mundial está inserida em uma sociedade da informação, que se traduz em agrupamento de nações que convivem em estado gregário e que em colaboração mútua, tem como seu padrão comum se nortearem pela informação como seu maior ativo, e que possuem como principal ferramenta para formarem um regime global de acesso à informação: a internet. (Machado; Barreto; Peccicacco, 2024).

A expansão da Internet das Coisas (IoT) conecta uma variedade de dispositivos, desde eletrodomésticos até carros, transformando nossas interações com o ambiente.

> Na relação custo x benefício da automação em residências, Alves e Mota (2003) afirmam que o investimento implica no usufruto imediato dos benefícios das diversas funcionalidades instaladas e, posteriormente, auxilia na capitalização da valorização do investimento em contraponto com a possível desvalorização inerente a um edifício desatualizado, sem condições de adaptar-se às necessidades tecnológicas de cada momento. Assim, além dos aspectos relacionados à sustentabilidade, também podem ser exploradas as melhorias no conforto. (Deboni; Alvarez; Bissoli, 2011, p. 2).

De acordo com Barreto e Machado, nos últimos anos houve uma imensa adoção do uso de dispositivos eletrônicos como *notebooks, tablets e smartphones* e de inúmeros aplicativos que quase sempre podem ser "baixados" pela internet - o que caracteriza a IoT -, culminando em um grande compartilhamento de informações, ideias e conhecimento, além da possibilidade da prestação de serviços, que geram um disrupção, ou seja, a quebra de um paradigma e sua substituição por uma nova maneira de se realizar um serviço, por exemplo.(Barreto; Machado, 2020):

> Internet das coisas é: uma infraestrutura de rede dinâmica e global com capacidades de autoconfiguração baseadas em protocolos de comunicação padronizados e interoperáveis nos quais as 'coisas' físicas e virtuais tem identidades, atributos físicos, personalidades virtuais, usam interfaces inteligentes e são completamente integradas na rede de informação. Na IoT, é esperado que as 'coisas' se tornem participantes ativas dos negócios e dos processos informacionais e sociais nos quais eles são capazes de interagir e comunicar-se entre eles e com o ambiente através da troca de dados e informação percebida sobre o ambiente, enquanto reagem de forma autônoma aos eventos do 'mundo físico/real' e o influenciam ao iniciar processos que engatilham ações e criam serviços com ou sem intervenção humana direta. Interfaces na forma de serviços facilitam as interações com as 'coisas inteligentes' na Internet,

> informar e alterar seus estados e qualquer informação associada a eles, levando em conta questões de segurança e privacidade. (Cerp IoT, 2009, p. 6).

Este estudo pretende discutir os benefícios, os riscos e as melhores práticas associadas ao uso desses dispositivos. A rápida adoção de dispositivos inteligentes oferece inúmeras vantagens, como automação e maior eficiência energética, mas também traz desafios críticos em termos de segurança e privacidade:

> Quando surge uma nova tecnologia ao mercado, traz consigo um novo vocabulário e, quando o assunto é residência inteligente, não é diferente: casa automática, casa inteligente, automação residencial, domótica, entre outros, são termos que fazem parte do universo de definições da Automação Residencial (Cecato, 2010, p. 12).

A disponibilização dos dados e das informações geram algumas discussões na esfera da intimidade e privacidade das pessoas naturais e jurídica. Quando tratamos de redes sociais, uma das mais famosas pelo seu uso, *Facebook*, tem sua plataforma um conteúdo inesgotável de informações e dados que, segundo a sua política de dados, há disposição expressa no tocante a utilização destes conteúdos com intuito de desenvolver serviços personalizados, a realização de pesquisas e resolução de problemas. À medida que mais dados pessoais são coletados e armazenados por esses dispositivos, aumenta a preocupação com o potencial de violações de dados e ataques cibernéticos.

> Como sempre, a segurança é fundamental para nós e para a nossa família. Portanto, somos nós que nos aprisionamos em nossas casas e, com o auxílio do sistema da casa inteligente, podemos prover muitas cenas de alerta. No caso de uma invasão, acendem-se todas as luzes internas e externas, proporcionando também sinais de alerta pisca-pisca, assim, assustando os invasores. E há ainda, uma integração no sistema telefônico conectado direto à polícia (ao qual se deve consultar previamente o órgão responsável), e também a função de criação de cenários adequados, no caso de uma viagem mais prolongada, ao qual, a casa acende e apaga as luzes, em horário previamente determinado (Cecato, 2010, p. 15).

A pesquisa acadêmica nesta área ainda está em desenvolvimento, e este resumo expandido visa contribuir para a compreensão desses desafios e propor soluções possíveis da seguinte maneira: Analisar os impactos dos equipamentos inteligentes na vida cotidiana, com foco nos aspectos de privacidade e segurança; Examinar o papel da IoT na automação residencial e nos dispositivos de uso pessoal; Avaliar as implicações para a privacidade dos dados gerados por equipamentos inteligentes; Investigar os riscos de segurança associados a esses dispositivos; Propor recomendações para o uso seguro e consciente dos equipamentos inteligentes. O resumo expandido foi baseado em uma revisão bibliográfica de estudos acadêmicos, estatísticas gráficas, podendo vir utilizar casos práticos. Importante destacar, o

levantamento feito SAP sobre as facilidades que as tecnologias trouxeram para as residências. Senão vejamos:



As perspectivas de crescimento de mercado por linha de produtos voltados para casas inteligentes tendem a crescer e refletir diretamente no mercado de aquisição de bens capazes de otimizar o bem-estar e facilitar o cotidiano das pessoas e famílias: Na sequência, traz-se outra pesquisa que aponta para o ranking, realizado em agosto de 2020, dos países no mercado de casas inteligentes. Aqui vemos a posição do Brasil em décimo primeiro lugar, o que chama atenção.



Destes dados é possível concluir que a aquisição dos equipamentos inteligentes vem em um crescimento exponencial, dado as facilidades que estas ferramentas permitem. Outro aspecto, é a adaptabilidade das famílias as novas tecnologias domésticas.

CONCLUSÃO

Conclui-se, brevemente que a nova maneira de organizar as riquezas, as corporações e suas relações com as informações veiculadas e constante fluxo informacional servem de produto de análise e comercialização, são novos padrões comportamentais que surgem nessa era digital. E com o Mundo modernizado em que vivemos, necessário também tratar da proteção em ambientes tecnológicos, a chamada infovigilância. Após as revelações de Snowden, o PLC

21/2014, que deu origem ao Marco Civil da Internet e que foi uma das prioridades do governo em 2013, foi aprovado com o intuito de garantir maior privacidade na rede mundial de computadores. Cabe salientar, então, que a Lei 12.965/2014 que regula direito, deveres e garantias dos usuários do world *wide web* no país, é um outro mecanismo contra a espionagem internacional.

> O texto da nova lei foi elaborado com base no documento "Princípios para a governança e o uso da internet", do Comitê Gestor da Internet no Brasil (CGI.br), organismo multissetorial responsável por integrar iniciativas de uso e desenvolvimento da internet brasileira. O documento é resultado de uma consulta pública, promovida entre 2009 e 2010, na qual foram arroladas mais de 800 contribuições de diferentes representantes da sociedade civil. Entre os principais eixos temáticos tratados pelo texto, e adotados pelo Marco Civil da Internet, estão a privacidade, a neutralidade da rede e a inimputabilidade da rede. Tais princípios garantiriam os direitos e liberdades democráticas de internautas frente a ações abusivas de governos (nacionais e estrangeiros) e empresas prestadoras de serviços. (Bezerra; Waltz, p. 162, 2014).

O resumo expandido proporcionou uma compreensão mais aprofundada dos impactos dos equipamentos inteligentes, tanto positivos quanto negativos.

> Uma residência inteligente agrega vários ambientes inteligentes contendo inúmeros dispositivos inteligentes [...] Desta forma, para se otimizar a relação entres usuário e equipamentos, é importante dividir o espaço físico em subespaços virtuais, proporcionando setores diferenciados com relação ao controle dos sistemas e padrões de sensoriamento. (Bolzani, 2004, p. 21-22).

Espera-se oferecer insights que ajudem a orientar consumidores, desenvolvedores e formuladores de políticas em direção a um uso mais seguro e eficiente dessas tecnologias. A expansão dos equipamentos inteligentes promete transformar a vida cotidiana, mas também apresenta desafios significativos, especialmente em termos de segurança e privacidade. Este artigo tem como objetivo fornecer um panorama detalhado desses impactos, além de sugerir estratégias para mitigar os riscos envolvidos.

REFERÊNCIAS

BEZERRA, Arthur Coelho; WALTZ, Igor. Privacidade, neutralidade e inimputabilidade da internet no brasil: avanços e deficiências no projeto do marco civil. **Revista Eptic Online**, Vol.16 n.2 p.161-175, mai-ago 2014.

BOLZANI, C. A. M. **Residências inteligentes.** São Paulo: Editora Livraria da Física, 2004.

CECATO, J. C. **Casa inteligente de baixo custo.** 2010. 32 f. Monografia (graduação) – Curso de Engenharia elétrica, Universidade São Francisco, 2010.

CERP IoT – **Internet of things European research cluster**. Internet of Things: Strategic Research Roadmap. 2009.

DEBONI, M. L.; ALVAREZ, C. E. de; BISSOLI, M. **Automação: uma ferramenta auxiliar na busca da sustentabilidade na construção civil**. Vitória, 2011. 10 p.

MACHADO, Ronny Max; BARRETO, Osmar Fernando Gonçalves. OS ASPECTOS TRABALHISTAS DO UBER E A INTERNET DAS COISAS. In: **Anais do Congresso Brasileiro de Processo Coletivo e Cidadania**. 2020. p. 1372-1386.

MACHADO, Ronny Max; PECCICACCO, Mariana; BARRETO, Osmar Fernando Gonçalves. A ESPIONAGEM INTERNACIONAL NO BRASIL: A TUTELA LEGAL DA SEGURANÇA NACIONAL. **Revista Jurídica OAB Tatuapé**, v. 3, n. 1, 2024.

PROJETO CONECTAR. **Como mensurar o mercado de Casas Inteligentes e Conectadas?** Disponível em: https://plataformaconectar.blogspot.com/2020/08/como-se-situa-o-brasil-no-mercado.html Acesso em: 13/10/2024

VALOR. N**ovas tecnologias vão aprimorar as casas inteligentes** Disponível em: https://valor.globo.com/publicacoes/suplementos/noticia/2022/12/19/novas-tecnologias-vao-aprimorar-as-casas-inteligentes.ghtml Acesso em: 13/10/2024.

7 Information Society and Law
FMU CENTRO UNIVERSITÁRIO

INTELIGÊNCIA ARTIFICIAL NO DIA A DIA COM ÉTICA E RESPONSABILIDADE NA ERA DIGITAL

ARTIFICIAL INTELLIGENCE IN EVERYDAY LIFE WITH ETHICS AND RESPONSIBILITY IN THE DIGITAL ERA

Sara Pereira Guimarães[1]

Resumo: Diversos setores da sociedade estão sendo alterados pela inteligente artificial (IA) e com isso, surgem questões éticas sobre responsabilidade, impacto social e privacidade. Além da eficiência, a IA precisa conter em seu escopo a justiça e a proteção dos dados em geral, enfrentando desafios como questões delicadas e sem total transparência. Para um uso mais responsável, deve haver uma regulamentação, educação, consciência e cooperação entre todos os setores. No futuro, a ética na IA deve se desenvolver de modo mais colaborativo e por regras mais rigorosas, a fim de garantir que a tecnologia promova um desenvolvimento mais justo e respeitoso com os direitos humanos.
Palavras-Chave: Ética; Responsabilidade; Privacidade; Justiça; Regulação.

Abstract: Several sectors of society are being changed by artificial intelligence (AI) and with this, ethical questions arise about responsibility, social impact and privacy. In addition to efficiency, AI needs to contain fairness and data protection in general in its scope, facing challenges such as sensitive issues and lack of complete transparency. For more responsible use, there must be reflection, education, awareness and cooperation between all sectors. In the future, ethics in AI must develop in a more collaborative way and through stricter rules, in order to ensure that the technology promotes fairer development that respects human rights.
Keywords: Ethic; Responsibility; Privacy; Justice; Regulation.

INTRODUÇÃO

A Inteligência Artificial (IA) tem ganhado força em diversos setores da sociedade, promovendo inovações que otimizam processos e melhoram a qualidade de vida. No entanto, à medida que essas tecnologias se tornam mais integradas ao cotidiano, surgem questões éticas complexas que demandam uma reflexão crítica. A aplicação de sistemas automatizados levanta preocupações sobre a responsabilidade na tomada de decisões e a proteção de dados pessoais, fundamental em um mundo cada vez mais digitalizado (JORDAN, Michael. "Artificial Intelligence: The Revolution Hasn't Happened Yet". AI & Society. HDSC, 2019). Disponível em: https://hdsr.mitpress.mit.edu/pub/wot7mkc1/release/10. Acesso em 31 out. 2024.

[1] Graduanda em Direito pela FMU - SP.

A ética da IA não se limita apenas à eficiência e à inovação; ela envolve também a consideração dos impactos sociais e morais das decisões tomadas por máquinas (RUSSELL & NORVIG. Artificial Intelligence: A Modern Approach. 4th Edition. Pearson Education, 2020). Nesse contexto, a responsabilidade torna-se um conceito central: quem é o responsável quando um sistema de IA comete um erro que resulta em danos? As respostas a essa pergunta são fundamentais para garantir que a IA não comprometa direitos individuais e a justiça social (BINNS, R. "Fairness in Machine Learning: Lessons from Political Philosophy". Proceedings of the 2018 Conference on Fairness, Accountability, and Transparency, 2018).

Além disso, a proteção de dados emerge como um imperativo ético e legal, à medida que a coleta e o processamento de grandes volumes de dados para IA aumentam o risco de violações de privacidade (CRAWFORD, Kate. Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence. Yale University Press, 2021). Leis como a Lei Geral de Proteção de Dados (LGPD) no Brasil e o Regulamento Geral sobre a Proteção de Dados (GDPR) na União Europeia estabelecem diretrizes rigorosas para o tratamento de dados, mas a eficácia dessas regulamentações depende de uma compreensão profunda dos desafios que a IA apresenta (BRASIL. Lei Geral de Proteção de Dados Pessoais LGPD, 2018) (UNIÃO EUROPEIA. Regulamento Geral sobre a Proteção de Dados GDPR, 2016).

Este artigo busca explorar a ligação entre ética, responsabilidade e proteção de dados em sistemas de IA, analisando os desafios que surgem na implementação de práticas responsáveis e na garantia da privacidade e da segurança dos dados dos usuários. A reflexão sobre esses temas é essencial para a construção de uma sociedade em que a tecnologia atue como aliada, respeitando os direitos humanos e promovendo um futuro mais igualitário e ético.

DISCUSSÕES E RESULTADOS

1. A Ética da Inteligência Artificial

A ética da inteligência artificial (IA) é um campo interdisciplinar que analisa as implicações morais, sociais e políticas do desenvolvimento e uso de tecnologias de IA. Com a crescente integração da IA em diversos aspectos da vida cotidiana, a discussão sobre sua ética se torna cada vez mais relevante. Este capítulo explora os princípios éticos que devem guiar a criação e implementação da IA, os desafios enfrentados na prática e a importância de uma abordagem centrada no ser humano.

Princípios Éticos da IA

Os princípios éticos da IA podem ser categorizados em várias áreas, cada uma abordando diferentes aspectos do desenvolvimento e uso dessas tecnologias. Os principais princípios incluem:

- Transparência: A IA deve ser desenvolvida de forma que seus processos e decisões sejam compreensíveis para os usuários. Isso implica na criação de sistemas que expliquem suas decisões de maneira clara, permitindo que os usuários entendam como e por que uma conclusão foi alcançada. (Princípios éticos da inteligência artificial (IA): navegando no universo digital com responsabilidade. Impacta, 2024. Disponível em:https://www.impacta.com.br/blog/principios-eticos-da-inteligencia-artificial/,2024). Acesso em: 31 out. 2024. (O que é IA ética?. IBM, 2024. Disponível em: https://www.ibm.com/br-pt/topics/ai-ethics). Acesso em 31 out. 2024.

- Justiça e Não Discriminação: É fundamental que os sistemas de IA não perpetuem ou aumentem discriminações existentes. Isso requer práticas que assegurem que a coleta de dados e os algoritmos utilizados sejam justos e equitativos, evitando preconceitos raciais, de gênero e socioeconômicos (Dez princípios para utilizar a inteligência artificial com ética. Centro De Ensino E Pesquisa, 2024. Disponível em: https://cep.jatai.ufg.br/n/115789-dez-principios-para-utilizar-a-inteligencia-artificial-com-etica). Acesso em 31 out. 2024. (Regras e usos éticos da Inteligência Artificial: conheça o código de ética da Weni. Weni, 2023. Disponível em: https://weni.ai/blog/codigo-de-etica-no-uso-de-ia/). Acesso em 31 out. 2024.

- Responsabilidade: A atribuição de responsabilidade é central na ética da IA. Quando um sistema automatizado toma uma decisão errada, é de suma importância determinar quem é responsável — seja o desenvolvedor, a empresa ou o próprio usuário. Essa responsabilidade deve ser clara a fim de garantir que as partes envolvidas possam ser responsabilizadas por seus atos.

- Privacidade: A proteção da privacidade dos indivíduos é essencial na ética da IA. As tecnologias frequentemente dependem da coleta e análise de grandes volumes de dados pessoais, levantando preocupações sobre como esses dados são utilizados e protegidos. É

imperativo que os desenvolvedores respeitem a privacidade dos usuários e cumpram legislações como a LGPD. (Ética da Inteligência Artificial (IA) no Brasil. Unesco, 2024. Disponível em: https://www.unesco.org/pt/fieldoffice/brasilia/expertise/artificial-intelligence-brazil). Acesso em 31 out. 2024.

Desafios Éticos

Apesar da clareza dos princípios éticos, sua implementação prática enfrenta diversos desafios:

- Algoritmos enviesados: Sistemas de IA podem conter muitas vezes vieses nos dados usados para treiná-los, resultando em discriminações em áreas sensíveis como crédito e justiça criminal, podendo aumentar o preconceito. A mitigação dessa problemática exige uma análise cuidadosa dos dados e técnicas para corrigir desequilíbrios.
- Dificuldade de Transparência: Muitos algoritmos, especialmente os baseados em aprendizado profundo, são considerados "caixas-pretas", dificultando a explicação de suas decisões. Isso pode gerar desconfiança entre os usuários.

- Riscos de Desemprego: A automação trazida pela IA pode resultar em perdas significativas de postos de emprego em vários setores. A ética da IA deve considerar o impacto social dessas tecnologias e promover abordagens que minimizem o desemprego, em que o empregado utilize a inteligência artificial como ferramenta para fazer o seu trabalho, e não a IA substituindo o trabalhador, quando possível.
- Abordagens Éticas

Para enfrentar os desafios éticos da IA, várias abordagens têm sido propostas:

- Governança e Regulação: A criação de regulamentações que orientem o desenvolvimento e uso da IA é crucial. Iniciativas como as diretrizes da Comissão Europeia, por exemplo, visam promover uma IA ética e responsável, estabelecendo normas claras para os desenvolvedores.
- Educação e Sensibilização: A formação de desenvolvedores, usuários e tomadores de decisão sobre as implicações éticas da IA é essencial. Promover uma cultura de responsabilidade ética nas organizações pode ajudar a criar um ambiente que priorize a ética na implementação tecnológica. (Dez princípios para utilizar a inteligência artificial com ética.

Centro De Ensino E Pesquisa, 2024. Disponível em: https://cep.jatai.ufg.br/n/115789-dez-principios-para-utilizar-a-inteligencia-artificial-com-etica). Acesso em 31 out. 2024.

- Colaboração Multissetorial: A ética da IA deve ser abordada colaborativamente, envolvendo academia, setor privado, governo e sociedade civil. Essa colaboração pode facilitar o desenvolvimento de melhores práticas e políticas que garantam benefícios amplos da IA.

2. Futuro da Ética na Inteligência Artificial

À medida que a inteligência artificial (IA) continua a se desenvolver e se integrar em diversos aspectos da vida cotidiana, o futuro da ética na IA apresenta tanto desafios quanto oportunidades. A evolução tecnológica, combinada com um crescente reconhecimento da importância da ética, moldará o cenário da IA nos próximos anos. Este capítulo discute algumas das principais tendências e previsões para a ética na IA.

Aumento da Regulação e Governança

Com a crescente preocupação sobre os impactos sociais e éticos da IA, espera-se que haja um aumento significativo na regulação e na governança dessas tecnologias. Governos e organizações internacionais estão se mobilizando para criar diretrizes e legislações que garantam o regulamento e desenvolvimento responsável da IA.

Essa tendência deve se intensificar, promovendo um ambiente regulatório que exija transparência, responsabilidade e equidade.

Desenvolvimento de Tecnologias Éticas

Outra previsão importante é o aumento do foco no desenvolvimento de tecnologias que incorporam princípios éticos desde sua concepção. Os pesquisadores e desenvolvedores estão cada vez mais conscientes da necessidade de projetar sistemas de IA que sejam justos, transparentes e responsáveis. Isso pode incluir a implementação de algoritmos que minimizem preconceitos e o uso de técnicas de aprendizado de máquina explicável, que ajudem a desmistificar o funcionamento da IA para os usuários (BINNS, R. "Fairness in Machine Learning: Lessons from Political Philosophy." Proceedings of the 2018 Conference on Fairness, Accountability, and Transparency, 2018).

Com o tempo, espera-se que a ética se torne uma parte integrante do ciclo de vida do desenvolvimento de software.

A Importância da Educação e Conscientização

A educação e a conscientização sobre ética na IA devem se expandir, não apenas entre os desenvolvedores, mas também entre os usuários e o público em geral. A formação de uma força de trabalho capacitada para entender os dilemas éticos associados à IA será crucial para o futuro. Espera-se que instituições acadêmicas e organizações profissionais incluam a ética da IA em seus currículos e treinamentos, promovendo uma cultura que valorize a responsabilidade ética no uso da tecnologia (CRAWFORD, Kate. "Atlas of AI: Power, Politics, and the Planetary Cost of Artificial Intelligence, 2021 "

Colaboração Entre Setores

O futuro da ética na IA também está ligado à colaboração entre diferentes setores da sociedade. A necessidade de um diálogo aberto entre governos, empresas, acadêmicos e a sociedade civil será vital para abordar questões complexas e garantir que as tecnologias atendam às necessidades e valores da sociedade. Essa colaboração pode levar à criação de fóruns e plataformas que promovam a discussão ética, permitindo uma abordagem mais inclusiva e representativa nas decisões relacionadas à IA.

CONCLUSÃO

A ética da inteligência artificial é um campo em constante evolução que se torna cada vez mais relevante à medida que a tecnologia avança e alcança aspectos fundamentais da sociedade. Este artigo explorou a ligação entre ética, responsabilidade e proteção de dados em sistemas automatizados, destacando a necessidade de um desenvolvimento responsável da IA. A implementação de princípios éticos, como transparência, justiça, responsabilidade e proteção da privacidade, é crucial para assegurar que as tecnologias sirvam ao bem comum e respeitem os direitos humanos (RUSSEL, Stuart. *Artificial Intelligence: A Modern Approach*. 4. ed. Pearson, 2020).

À medida que a sociedade avança na adoção da IA, é imperativo que as discussões éticas sejam contínuas e dinâmicas, envolvendo todos. A ética deve ser vista como uma parte integrante do ciclo de vida da tecnologia, e não como uma reflexão tardia. Somente assim, poderemos garantir que a inteligência artificial não apenas promova inovações, mas também contribua para um futuro mais justo, equitativo e respeitoso com todos os indivíduos.

REFERÊNCIAS

BINNS, Reuben. Fairness in machine learning: lessons from political philosophy. In: **Proceedings of the 2018 Conference on Fairness, Accountability, and Transparency**, 2018. Disponível em: https://dl.acm.org/doi/10.1145/3287560.3287598. Acesso em: 31 out. 2024.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 31 out. 2024.

CRAWFORD, Kate. **Atlas of AI**: Power, Politics, and the Planetary Costs of Artificial Intelligence. New Haven: Yale University Press, 2021.

DEZ princípios para utilizar a inteligência artificial com ética. **Centro de Ensino e Pesquisa**, 2024. Disponível em: https://cep.jatai.ufg.br/n/115789-dez-principios-para-utilizar-a-inteligencia-artificial-com-etica. Acesso em: 31 out. 2024.

IBM. **O que é IA ética?** IBM Brasil, 2024. Disponível em: https://www.ibm.com/br-pt/topics/ai-ethics. Acesso em: 31 out. 2024.

JORDAN, Michael I. Artificial Intelligence: the revolution hasn't happened yet. **Harvard Data Science Review**, v. 1, n. 1, 2019. Disponível em: https://hdsr.mitpress.mit.edu/pub/wot7mkc1/release/10. Acesso em: 31 out. 2024.

PRINCÍPIOS éticos da inteligência artificial (IA): navegando no universo digital com responsabilidade. Impacta, 2024. Disponível em: https://www.impacta.com.br/blog/principios-eticos-da-inteligencia-artificial/. Acesso em: 31 out. 2024.

REGULAMENTO (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Regulamento Geral sobre a Proteção de Dados (GDPR). União Europeia. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 31 out. 2024.

RUSSELL, Stuart; NORVIG, Peter. **Artificial Intelligence**: a modern approach. 4. ed. Boston: Pearson Education, 2020.

UNESCO. **Ética da Inteligência Artificial (IA) no Brasil**. Brasília: Unesco, 2024. Disponível em: https://www.unesco.org/pt/fieldoffice/brasilia/expertise/artificial-intelligence-brazil. Acesso em: 31 out. 2024.

WENI. Regras e usos éticos da Inteligência Artificial: conheça o código de ética da Weni. Weni, 2023. Disponível em: https://weni.ai/blog/codigo-de-etica-no-uso-de-ia/. Acesso em: 31 out. 2024.

7 Information Society and Law
FMU CENTRO UNIVERSITÁRIO

INTELIGÊNCIA ARTIFICIAL E GOVERNANÇA - UMA NECESSIDADE GLOBAL

ARTIFICIAL INTELLIGENCE AND GOVERNANCE - A GLOBAL NECESSITY

Flavio Cesar Vasconcellos Ferreira[1]

Resumo: Através deste resumo expandido, buscou-se demonstrar que a evolução das aplicações da Inteligência Artificial tomou proporções irreversíveis no cotidiano dos indivíduos em todo o mundo e, consequentemente, a coleta, tratamento, uso e o compartilhamento de dados também alcançaram uma escala global. Empresas e desenvolvedores de Inteligência Artificial armazenam e comercializam dados de indivíduos como um ativo importante para os negócios, abrindo a possibilidade de utilizações não consentidas e manipulações em massa. Questões éticas passaram a integrar as discussões acerca dos limites e dos riscos que cercam a utilização dos sistemas de Inteligência Artificial, a proteção dos dados e as responsabilizações judiciais em casos de vazamento, mau uso ou roubo de dados. Ao examinar algumas propostas para regulamentações, este trabalho procurou contribuir para a discussão, trazendo a visão da governança como uma forma de auxiliar na supervisão, responsabilização e imposição de limites para as aplicações da Inteligência Artificial, de modo que os riscos de má utilização desses sistemas inteligentes sejam mitigados por meio do controle, da supervisão e da responsabilização de humanos.
Palavras-Chave: Inteligência Artificial; Governança; Regulamentação; Privacidade; Ética.

Abstract: Through this extended summary, it sought to demonstrate that the evolution of Artificial Intelligence applications has taken on irreversible proportions in the daily lives of individuals worldwide. Consequently, the collection, processing, use, and sharing of data have also reached a global scale. Companies and developers of Artificial Intelligence store and trade individual data as an important asset for business, opening up the possibility of non-consensual uses and mass manipulations. Ethical issues have become part of the discussions regarding the limits and risks surrounding the use of Artificial Intelligence systems, data protection, and legal liabilities in cases of data breaches, misuse, or theft. By examining some proposals for regulations, this paper aimed to contribute to the discussion by bringing the perspective of governance as a way to assist in supervision, accountability, and the imposition of limits on the applications of Artificial Intelligence, so that the risks of misuse of these intelligent systems are mitigated through control, supervision, and accountability of humans.
Keywords: Artificial Intelligence; Governance; Regulation; Privacy; Ethics.

[1] Administrador, Especialista em Compliance e Mestrando em Governança Corporativa pela FMU/Unifesp.

INTRODUÇÃO

Matéria do jornal norte-americano The New York Times, publicada em 16 de setembro de 2024, reportava que um grupo internacional de pesquisadores da Inteligência Artificial (IA) se reuniu para expressar suas preocupações com os avanços da tecnologia que auxiliaram a construir e que, segundo os cientistas, os avanços sinalizam que poderiam causar danos severos à sociedade.

Reunindo pesquisadores nos Estados Unidos, China, Grã-Bretanha, Cingapura, Canadá, entre outros países, o comunicado conjunto afirmou que a IA ultrapassaria a capacidade de seus criadores e, a consequente perda de controle humano, levaria a resultados severos para a humanidade. Os pesquisadores sugerem que os países deveriam articular a criação de um sistema global de supervisão que verificasse os riscos potencialmente graves apresentados pela tecnologia em rápida evolução.

De acordo com a reportagem, no início do mês de setembro de 2024, em Veneza, na Itália, pesquisadores de todo o mundo realizaram a terceira reunião do Diálogo Internacional sobre Segurança em I.A., que resultou em um alerta para que os governos saibam o que está em curso nos laboratórios de pesquisa e nas empresas que trabalham com sistemas de I.A. A proposta dos pesquisadores é pelo estabelecimento de autoridades de segurança em I.A. para acompanhar o desenvolvimento de sistemas dentro de suas fronteiras. Estas autoridades trabalhariam de forma articulada para o estabelecimento de sinais de que um sistema de I.A. poderia copiar-se ou ludibriar intencionalmente seus criadores ou controladores, coordenados por um corpo internacional.

Ainda segundo a matéria jornalística, movimentos governamentais neste sentido já ocorrem em países como os Estados Unidos, China e na Grã-Bretanha. O governo americano expediu uma ordem executiva exigindo que as empresas relatassem ao governo federal dos riscos que seus sistemas de I.A. poderiam representar, como a criação de armas de destruição em massa ou o potencial para uso em ações de terrorismo. A China possui um marco de segurança para as aplicações de I.A. e a Grã-Bretanha tem uma iniciativa mais ampla, reunindo oficiais de 28 países que concordaram em cooperar na avaliação dos riscos da I.A., mas ainda não houve a definição de políticas específicas para esta coordenação.

Como o avanço da tecnologia da I.A. ocorre rapidamente, é mais difícil que empresas e governos consigam abordá-la de forma isolada, por isso, a cooperação internacional é crucial para a segurança global, conclui a reportagem do The New York Times.

Justifica-se este estudo pela evidenciação de que a evolução segura da I.A. passa pela conjugação da proteção dos direitos fundamentais, como a privacidade e a não discriminação, com o fomento à inovação para pesquisas, máquinas, tecnologias e avanços que viabilizem soluções para problemas complexos. E a problemática proposta questiona "Como os mecanismos de governança poderiam se inserir na evolução segura das aplicações de I.A.?".

Para atender ao proposto, a pesquisa documental foi utilizada como método de trabalho.

DISCUSSÕES E RESULTADOS

Houve um avanço legislativo na União Europeia que posiciona o bloco na vanguarda regulatória da I.A. Aprovado pelo Parlamento Europeu em 21 de maio de 2024, a Lei de Inteligência Artificial da União Europeia (IA Act) propõe uma abordagem baseada em riscos para a segurança, transparência e respeito aos direitos fundamentais no desenvolvimento e aplicação dos sistemas de I.A.

Os sistemas classificados como de risco inaceitável são as aplicações de I.A. consideradas como forma de ameaça ou de controle do indivíduo e, por estas características, serão proibidas. Aqui estão as aplicações para **manipulação cognitiva de comportamentos e para classificação social, como** os sistemas que utilizam **dados biométricos** para classificar o indivíduo por raça, religião ou orientação sexual, não permitidas na União Europeia.

Os sistemas de I.A. que apresentem um **risco considerado elevado são aqueles que afetam negativamente a segurança ou os direitos fundamentais e estarão sujeitos a um conjunto de requisitos e obrigações para que sejam autorizados a acessar o mercado da União Europeia. Os sistemas considerados de risco limitado deverão atender a algumas obrigações para transparência. E entre as aplicações consideradas como de risco mínimo estão os jogos com I.A. e os filtros de spam.**

Prevê ainda a legislação da União Europeia que os sistemas de I.A. serão avaliados antes de serem disponibilizados ao público e durante todo o seu ciclo de vida, bem como

poderão os indivíduos apresentarem queixas junto às autoridades nacionais competentes contra os sistemas que violem os termos da legislação.

Segundo o Parlamento Europeu, a IA Act visa a promoção, o desenvolvimento e a utilização de sistemas de I.A. **seguros** e confiáveis, que resguardem o respeito aos **direitos fundamentais** dos cidadãos e estimulem o investimento e a inovação na União Europeia. A IA Act é restrita aos países do bloco e prevê algumas isenções, como para os sistemas exclusivamente militares e de defesa e os sistemas de investigação criminal.

Há também a previsão de uma estrutura de governança para apoiar a efetividade da IA Act na União Europeia, como a criação de uma comissão para fiscalizar o cumprimento regulatório na região, um painel científico independente para apoiar a execução, um comitê de aconselhamento à comissão e aos Estados-Membros e um fórum consultivo para oferecer conhecimentos técnicos.

As primeiras críticas à proposta regulatória da I.A. na União Europeia partem da abordagem da gestão de riscos que, usualmente, atua na medição, mitigação e aceitação dos riscos em favor de algum benefício. Ocorre que os avanços da I.A., além de rápidos, contemplam inúmeras áreas possíveis de aplicação e replicação. Isso dificulta a classificação dos riscos conforme proposta, uma vez que as aplicações, desdobramentos e consequências da I.A. são ilimitados. A utilização da gestão de riscos pode desconsiderar em sua análise os eventuais danos oriundos de direitos fundamentais, como os danos à dignidade humana, à liberdade e à igualdade e os danos de mais complexa mensuração prévia, como as questões de cunho emocional e social.

ÉTICA E AS APLICAÇÕES DE INTELIGÊNCIA ARTIFICIAL

Nas preocupações éticas derivadas das aplicações de I.A. encontram-se, por exemplo, os impactos sobre a privacidade e a coleta ostensiva, armazenamento e utilização de dados captados por dispositivos integrados à vida cotidiana, como aplicativos de segundo plano em smartphones, smartwatches e assistentes virtuais, que permanentemente coletam informações e podem gerar vulnerabilidades pelos potenciais violações de privacidade resultantes deste tipo de vigilância virtual.

A complexidade ética das aplicações de I.A. passa pela pelo fato de que os dados e as informações pessoais converteram-se em um ativo importante das empresas de tecnologia, do

desenvolvimento tecnológico e da economia. As legislações dos vários países sobre a proteção de dados renovaram a importância da atenção à privacidade e da necessidade do controle sobre a utilização de dados pessoais.

No ambiente regulatório brasileiro, a Lei nº 13.709/18, Lei Geral de Proteção de Dados, LGPD, estabeleceu em seu artigo vigésimo o direito do titular dos dados solicitar a revisão de decisões tomadas por tratamento automatizado de dados pessoais que afetem seus interesses, como decisões de consumo, de crédito ou de aspectos de sua personalidade. Tal previsão legal se mostra ainda mais relevante diante dos avanços verificados e previstos da I.A. que, conforme visto, caminha na direção da tomada de decisões autônomas com frequência cada vez maior. No entanto, verifica-se que não há clareza de que a revisão deva ser promovida obrigatoriamente por pessoa natural, o que permite interpretações divergentes do exercício do direito à revisão das decisões automatizadas.

É certo que as decisões humanas são influenciadas por variáveis diversas e que contém vieses, inclusive inconscientes, mas é igualmente seguro ponderar que decisões automatizadas não contenham critérios outros que não os originalmente concebidos, abrindo espaço para a criação de uma aprendizagem de máquina que pode comprometer ou ignorar direitos humanos fundamentais por não reconhecerem limites éticos.

RISCOS

Outro aspecto a ser considerado é o de ocorrência de quebras na segurança dos dados que permitam acessos não autorizados de forma acidental ou mesmo através de ações ilícitas deliberadas e que resultem na obtenção, manipulação ou divulgação dos dados armazenados. E como grande parte das atividades cotidianas ocorrem através de meios digitais, há maior e constante coleta de dados do indivíduo em poder das organizações e das tecnologias de I.A. Em caso de quebras na segurança dos dados, quanto maior a exposição dos dados pessoais, maiores poderão se tornar os riscos de manipulações ou de limitações do exercício dos direitos fundamentais, podendo mesmo alcançar o cerceamento de certos direitos.

De Sá e De Lima (2020) trazem questionamentos acerca da responsabilização em caso de danos ou de violações de direitos decorrentes do desenvolvimento e do emprego da I.A.

> Primeiramente, sobre quem recai a responsabilidade jurídica? Sobre o cientista, que é o 'pai' da tecnologia? Sobre o proprietário da máquina inteligente? Sobre a pessoa que está utilizando e monitorando o sistema de IA? Sobre a pessoa que determina a qual propósito a máquina deverá servir? Ou seria possível conferir personalidade jurídica

> aos robôs, autônomos e sistemas de IA, de modo a imputar-lhes o dever de ressarcir danos? (De Sá; De Lima, 2020, p. 240).

E continuam as autoras, trazendo questionamentos de outros tópicos relevantes acerca da responsabilização jurídica:

> Como se faria a compensação do dano ou da violação de direito? Qual a natureza dessa responsabilidade? Deve ser promulgada lei prevendo novos tipos penais? E, caso se estenda a todos os participantes da cadeia, que se inicia com a concepção da máquina e finda com sua utilização, a responsabilização patrimonial deve ser solidária ou fracionária? (De Sá; De Lima, 2020, p. 240).

Observamos o desenvolvimento tecnológico e econômico global, fomentando a inovação, a livre iniciativa, a livre concorrência. Ao mesmo tempo, observamos o crescimento das preocupações com o respeito a privacidade, a informação, a liberdade de expressão e de opinião, a inviolabilidade da intimidade, da honra e da imagem.

O avanço e a disseminação da I.A. tangenciam os direitos humanos e a ética na responsabilização e proteção dos dados coletados, armazenados e utilizados para os mais diversos fins, em especial nas tomadas de decisões automatizadas e os riscos decorrentes. Os sistemas de I.A. impactam cada vez mais aspectos da sociedade, desde a privacidade pessoal até a segurança pública, colocando as implicações éticas e de direitos humanos como preocupações críticas que demandam ações imediatas.

A ESTRUTURA DE GOVERNANÇA APLICADA À INTELIGÊNCIA ARTIFICIAL

Hammad Raza, é Engenheiro da Computação e pesquisador na National College of Business Administration & Economics, no Paquistão e publicou em outubro de 2024 um artigo acadêmico ponderando a adoção de uma estrutura de governança eficaz para abordar tais desafios e estabelecer estruturas que protejam os direitos individuais, promovam a transparência e garantam a responsabilização em sistemas de I.A. Para Raza (2024), as considerações de direitos humanos para uma governança de I.A. envolvem a proteção da privacidade, a prevenção da discriminação e a garantia da justiça em processos automatizados de tomada de decisão, constituindo estes fatores que determinarão a confiabilidade em sistemas de I.A.

Raza defende que a estrutura de governança para sistemas de I.A. envolva a criação de mecanismos para auditoria de algoritmos, a divulgação de fontes de dados e de metodologias nas decisões automatizadas como forma de construir a confiança pública e permitir a supervisão

humana das decisões dos sistemas de I.A. Além destes atributos, a estrutura de governança devem incluir claros mecanismos de responsabilização, permitindo que as partes interessadas apresentem queixas e que eventuais danos causados pelas aplicações de I.A. sejam rapidamente detidos e reparados.

A estruturação desta governança inclui o estabelecimento de responsabilidades para desenvolvedores e operadores de I.A., priorizando a proteção da privacidade, transparência, justiça e responsabilização. As estruturas de governança devem assegurar que os sistemas de I.A. sejam implantados e atuem na defesa dos direitos fundamentais, ou seja, impondo limitações e supervisão para as decisões automatizadas de I.A. através da adoção de mecanismos claros e rigorosos protocolos de segurança contra violações, uso indevido e proteção de dados.

Uma das bases para a governança da I.A. começa pelos mecanismos de consentimento para a coleta, uso e compartilhamento de dados. O indivíduo deve ser claramente informado sobre os dados que serão coletados, como serão utilizados, quem terá acesso a eles e, se consentir a utilização, o consentimento deve ser facilmente revogado a qualquer instante, conferindo ao indivíduo a possibilidade de controle sobre seus próprios dados.

Princípios de minimização de dados e limitação de finalidade devem ser observados. Os sistemas de I.A. devem coletar somente os dados essenciais para seus objetivos específicos e não devem manter os dados além do período necessário a sua finalidade. Os sistemas de I.A. devem ser desenvolvidos tendo a privacidade por padrão e incorporados desde o desenvolvimento, assegurando que a privacidade esteja integrada aos processos desde sua concepção.

CONCLUSÃO

Em conclusão, a proposta de Raza é que uma estrutura de governança em I.A. é urgente para assegurar a transparência nas operações automatizadas e que a educação das partes interessadas através de uma estrutura de regramento apoiaria o estabelecimento de limites éticos e legais e a previsão de responsabilizações. A governança eficaz da I.A. requer uma abordagem abrangente para estabelecer o respeito aos direitos humanos, promover justiça e manter padrões éticos.

Braga et al (2024) relatam um modelo de governança em três níveis, sendo o primeiro no plano da infraestrutura técnica para acessos seguros, funcionais e robustos em termos de estabilidade e alcance. A segunda camada de governança recai sobre as aplicações e serviços disponibilizados de forma virtual, onde se situam as estruturas para a privacidade de dados, cibersegurança e livre concorrência, sendo necessárias permanente avaliação e revisões. A terceira camada se relaciona com os usuários, empresas, governos e a sociedade em geral para assegurar mecanismos de proteção e responsabilização por danos relacionados ao emprego da I.A. Concluem os autores que a governança para a regulamentação de protocolos, algoritmos, softwares e infraestrutura é algo complexo e em evolução, que envolve aspectos técnicos, políticos, econômicos, jurídicos, sociais, culturais e exigirá a participação de organismos globais, governos, empresas e sociedade civil. Não será uma solução centralizadora ou hierarquizada, mas distribuída, colaborativa e articulada conforme os riscos forem evoluindo.

Os sistemas de valores da governança regulam o relacionamento entre as partes, os propósitos estratégicos, a estrutura de poder e as práticas para a gestão. A aplicação dos princípios de equidade entre as partes, transparência, prestação de informações e a questão da conformidade com os regramentos aparecem aplicadas de forma customizada para contribuir com a necessidade da evolução segura da I.A. A inserção da governança nesta nova era do desenvolvimento da humanidade oferece a possibilidade de segurança para a disciplina e para a adequada aplicação da I.A., bem como a previsão de responsabilização e de sanções para os que optarem por desvios do caminho que a coletividade global entender como seguro e ético.

REFERÊNCIAS

BORGES, Davi Wesley, et al. As Leis de Proteção de Dados e Sua Aplicação ao Treinamento de IA. **Revista Foco**, 2024, 17.10: e6614-e6614.

BRAGA, Julião, et al. Como a Governança de Múltiplas Partes Interessadas Pode Moldar a IA Responsável. **OSF Preprint**, Março de 2024. Disponível em: https://osf.io/preprints/osf/zeg9m. Acesso em: 28 outubro 2024.

CONSELHO DA UNIÃO EUROPEIA. Regulamento Inteligência Artificial (IA): Conselho dá luz verde final às primeiras regras do mundo em matéria de IA. **Comunicado de Imprensa**. Disponível em: https://www.consilium.europa.eu/pt/press/press-releases/2024/05/21/artificial-intelligence-ai-act-council-gives-final-green-light-to-the-first-worldwide-rules-on-ai/. Acesso em: 30 outubro 2024.

DE SÁ, Maria de Fátima Freire; DE LIMA, Taisa Maria Macena. Inteligência artificial e Lei Geral de Proteção de Dados Pessoais: o direito à explicação nas decisões automatizadas. **Revista Brasileira de Direito Civil**, 2020, 26.04: 227-227.

LEI DE INTELIGÊNCIA ARTIFICIAL DA UNIÃO EUROPEIA (IA Act). **Website dedicado**. Disponível em: https://artificialintelligenceact.eu/. Acesso em: 29 outubro 2024.

RAZA, Hammad. Data Ethics and Human Rights: Designing Robust Governance Structures for AI Systems. **Researchgate.net**. 2024. 10.13140/RG.2.2.11535.80805.

TOBIN, Meaghan. A.I. Pioneers Call for Protections Against 'Catastrophic Risks'. **The New York Times**. Nova Iorque, EUA. No 60.309, edição de 16 de outubro de 2024. Disponível em https://www.nytimes.com/2024/09/16/business/china-ai-safety.html?searchResultPosition=4. Acesso em: 25 outubro 2024.

7 Information Society and Law
FMU CENTRO UNIVERSITÁRIO

TEORIA CRÍTICA DO DIREITO: DESVELANDO AS ESTRUTURAS DE PODER E EMANCIPAÇÃO NA ERA DIGITAL

CRITICAL THEORY OF LAW: UNCOVERING THE STRUCTURES OF POWER AND EMANCIPATION IN THE DIGITAL AGE

Edielma Rocha Dutra[1]; Paula Aline Aguiar Gozi[2]

Resumo: O texto analisa a Teoria Crítica do Direito, inspirada por Karl Marx e pensadores da Escola de Frankfurt, como Horkheimer e Adorno. Os autores propõem que o direito reflete as relações sociais e econômicas, servindo muitas vezes aos interesses de grupos dominantes. A pesquisa utiliza uma abordagem teórica e crítica, destacando a interdependência entre teoria e prática, e a necessidade de desafiar estruturas de dominação, especialmente em um mundo digitalizado.
Palavras-chave: Teoria Crítica do Direito; relações sociais; relações econômicas; Inteligência Artificial; ética.

Abstract: The text analyzes the Critical Theory of Law, inspired by Karl Marx and thinkers from the Frankfurt School, such as Horkheimer and Adorno. They propose that law reflects social and economic relations, often serving the interests of dominant groups. The research uses a theoretical and critical approach, highlighting the interdependence between theory and practice, and the need to challenge structures of domination, especially in a digitalized world.
Keywords: Critical Theory of Law; social relations; economic relations; Artificial Intelligence; ethical.

INTRODUÇÃO

A Teoria Crítica do Direito, inspirada nas ideias de Karl Marx, oferece uma perspectiva crítica sobre o direito como reflexo das relações sociais e econômicas, frequentemente servindo aos interesses dos grupos dominantes. Este estudo explora como essa teoria pode reinterpretar o direito para promover a emancipação humana, especialmente em um mundo digitalizado.

[1] Graduada pela Universidade Católica de Santos (UNISANTOS) Pós-graduada em Direito Processual Penal pelo Instituto Damásio de Direito/IBMEC. Pós-graduanda em Direito Penal e Criminologia na PUC Rio Grande do Sul. Mestranda em Direito da Sociedade da Informação pelo Centro Universitário das Faculdades Metropolitanas Unidas (FMU).
[2] Advogada. Mestranda em Direito da Sociedade da Informação pelo Centro Universitário das Faculdades Metropolitanas Unidas (FMU). Pós-Graduada em Direito do Trabalho, Processo do Trabalho e Práticas Trabalhistas e Pós Graduanda em Direito das Pessoas Vulneráveis. Bacharel em Direito pela Escola Paulista de Direito (EPD). E-mail: paulaalinegozi@gmail.com.

Com base nas contribuições de pensadores como Max Horkheimer, Theodor Adorno e Jürgen Habermas, essa pesquisa analisa a interdependência entre teoria e prática, destacando a necessidade de uma abordagem crítica para desafiar estruturas de poder e dominação. Este trabalho visa contribuir para o debate sobre a relevância da Teoria Crítica do Direito na sociedade contemporânea, enfatizando sua importância para promover justiça social, igualdade e direitos humanos.

DISCUSSÕES E RESULTADOS

Este trabalho explora a Teoria Crítica do Direito, inspirada no modelo crítico de Karl Marx, que destacou as falhas das formas utópicas de socialismo e das análises descritivas da economia política clássica. A pesquisa aborda o problema de como a teoria crítica pode reinterpretar o direito como um reflexo das relações sociais e econômicas, frequentemente servindo aos interesses dos grupos dominantes.

A metodologia utilizada é uma análise teórica e crítica da literatura existente, destacando a interdependência entre teoria e prática e a conexão entre sujeito e objeto em uma perspectiva histórico-social. Os objetivos incluem identificar planos ideológicos de dominação e explorar as potencialidades e limites para a emancipação humana.

A justificativa para o estudo reside na necessidade de uma crítica ao status quo que desafie os arranjos de dominação nas relações humanas, especialmente em um mundo digitalizado.

Uma característica central da Teoria Crítica é a sua abordagem que, ao contrário do método teórico tradicional, concebe teoria e prática como interdependentes, conectando sujeito e objeto em uma perspectiva histórico social concreta. Isso permite a identificação de planos ideológicos de dominação, bem como das potencialidades e limites para a emancipação humana presentes no contexto social. A Teoria Crítica do Direito, enraizada nas ideias do Marxismo e nas obras de pensadores da Escola de Frankfurt, como Max Horkheimer e Theodor Adorno, busca desvelar as relações de poder e dominação que permeiam as estruturas legais. Diferente das abordagens tradicionais que veem o direito como um sistema neutro e objetivo, a teoria crítica o interpreta como um reflexo das relações sociais e econômicas, muitas vezes servindo aos interesses dos grupos dominantes. A teoria crítica é comumente associada à “Escola de Frankfurt” por diversos estudiosos.

No entanto, conforme explica a socióloga Bárbara Freitag, o conceito de teoria crítica foi especificamente desenvolvido por Max Horkheimer, sendo que tal associação se deu especialmente após a publicação dos trabalhos mais influentes, entre outros, de Adorno e Habermas. Foi apenas em 1930, durante seu discurso de posse como diretor do Instituto para a Pesquisa Social, que Horkheimer delineou o que viria a ser um programa para uma teoria crítica da sociedade. Assim, a expressão "teoria crítica" foi cunhada por Horkheimer e entendida de maneira específica: como um conhecimento voltado para a ação, em vez de uma busca por pureza ou neutralidade (FREITAG, 1994). Os primeiros textos em que Horkheimer formulou sua teoria crítica do direito foram “A presente situação da filosofia social e as tarefas de um Instituto de Pesquisa Social”, de 1931, e “Teoria tradicional e teoria crítica”, de 1937. Já nos anos 1990, Horkheimer, ao abordar o problema da verdade, desenvolve a ideia de que a teoria crítica está alinhada com os interesses específicos de certos grupos sociais, conforme ele explicou: “Os grandes sistemas de filosofia europeia eram sempre destinados a uma elite educada e não funcionavam diante das necessidades psíquicas daquela parcela de cidadãos e camponeses em vias de empobrecimento e aviltamento social, os quais, por outro lado, estão ligados necessariamente, pela educação, pelo trabalho e pela esperança, a esta forma de sociedade e não conseguem acreditar na sua transitoriedade” (HORKHEIMER, 1990, p.144).

Como Marx observou, o conflito na sociedade não é com seu conceito ideal, mas ocorre internamente, refletindo sua divisão em classes sociais (MARX, 1843). Dessa forma, a teoria crítica avança além de uma crítica baseada em padrões éticos, normas ou princípios que podem ser externos e que pressupõem a vida social ou são a priori. Assim, Horkheimer, ao conceber a teoria crítica, a defende como uma crítica ao status quo, escolhendo como seus agentes todos aqueles interessados em se libertar dos arranjos de dominação presentes nas relações humanas. Ao abordar o problema da verdade, ele formula a ideia de que a teoria crítica reflete os interesses específicos de certos grupos sociais. A teoria crítica é concebida como uma forma de ação, em contraste com a teoria tradicional, que busca a pureza. A ciência é percebida como uma força produtiva e uma relação social de produção que pode, ou não, legitimar o status quo. Horkheimer questiona qual é o potencial revolucionário do processo de racionalização. Ele reconhece que a teoria tradicional faz parte da totalidade social e é importante para o desenvolvimento das lutas sociais, assim como para a teoria e práxis críticas. Assim, na nova formulação, a teoria crítica deveria interagir reciprocamente com a teoria tradicional, de modo

a exercer uma influência libertadora e ser capaz de oferecer uma compreensão do tempo presente. Para a teoria crítica, a ação deve ser cuidadosamente ponderada, avaliada e julgada pela teoria, que é vista como uma mediação da prática. Assim, a teoria crítica se transforma em um aspecto da prática adequada, de acordo com os interesses de seus agentes, que podem estar em tensão com a perspectiva teórica. Nesse contexto, Horkheimer abordou o desafio de superar uma dialética meramente conceitual, buscando realizar a razão nas relações sociais e desenvolver um autoconhecimento da realidade, com o objetivo de identificar as condições para alcançar os ideais de liberdade, autonomia e emancipação humana promovidos pela sociedade burguesa. Ele propõe uma solução para esse problema através da reorientação da teoria tradicional, adotando um comportamento crítico e uma orientação voltada para a emancipação. Ludwig Wiesengrund-Adorno, em "Dialética negativa" (2009), também contribui na abordagem crítica do direito. Primeiramente, porque aborda de maneira eficaz uma crítica frequentemente direcionada à análise marxista, que é acusada de empregar um método que se limita a uma análise economicista do direito, sem levar em conta características superestruturais, como sua expressão normativa, por exemplo. O direito é introduzido pela primeira vez na terceira parte da obra, durante o desenvolvimento do modelo Liberdade. De acordo com Adorno, isso representa uma contribuição à metacrítica da razão prática. Neste modelo, o autor oferece uma crítica incisiva à noção de liberdade, especialmente como foi desenvolvida por Immanuel Kant. No trecho intitulado "Discurso em defesa da ordem", Adorno comenta:

> O fato de precisar haver liberdade é a injúria mais extrema do sujeito autônomo fundador do direito. O conteúdo de sua própria liberdade - da identidade que anexou tudo aquilo que não é mais idêntico - equivale à necessidade, à lei, ao domínio absoluto. (ADORNO, 2009, p. 210).

Ademais, Adorno também faz uma digressão sobre a dialética em Hegel, em que demonstra que o direito possui uma certa centralidade no que diz respeito à irracionalidade aparentemente racional que caracteriza a lógica da sociedade capitalista. O aspecto mais destacado, no entanto, está na maneira como Adorno aborda a transformação do princípio de equivalência em uma norma que uniformiza todos os indivíduos. Essa equivalência se converte em igualdade formal, um processo que ignora as diferenças específicas de cada indivíduo. Paradoxalmente, esse movimento sustenta as estruturas de desigualdade, ao mesmo tempo que as esconde sob a aparência de isonomia formal. Assim, a norma jurídica surge como impulsionadora e perpetuadora do mito fundamental da sociedade mercantil, uma narrativa

ilusória que afirma que todos são naturalmente iguais. O caráter distintivo da norma jurídica reside em criar um espaço significativo onde tudo o que não se encaixa em seus esquemas abstratos é excluído, por ser considerado sem sentido. As experiências específicas, mais relacionadas aos valores de uso do que aos valores de troca, são rejeitadas pela norma e, portanto, excluídas do domínio jurídico como algo simplesmente não jurídico. Adorno aborda também a questão de que o princípio de identidade, que impõe sua lógica à própria estrutura do pensamento, possui um fundamento material.

Dado que a Dialética Negativa se propõe como uma dialética materialista, é necessário investigar o fundamento oculto desse modo de articulação da realidade e revelá-lo. Apenas dessa forma pode se qualificar como uma ontologia do estado falso. Jüngen Habermas entende o projeto da Ilustração e, juntamente com Max Weber, identifica os processos de racionalização cultural e social, bem como suas reduções à racionalidade estratégica e instrumental. Na visão de Habermas, a sociedade é dividida em mundo da vida e sistema, onde predominam as ações comunicativas e as ações estratégicas e instrumentais, respectivamente. Contrariando o que se poderia supor, Habermas não advoga pela eliminação do sistema, nem da instrumentalidade que o caracteriza, pois o sistema é vital para a reprodução material do mundo da vida. Em vez disso, ele sugere uma inversão na ordem de comando societária, de forma que o mundo da vida passe a orientar o sistema, sem comprometer a essencial reprodução material. Percorrendo os ideais republicano e liberal de democracia, Habermas elabora sua proposta de democracia deliberativa, que se fundamenta na ética discursiva e na presença de direitos e princípios fundamentais. Esses elementos asseguram a formação discursiva da opinião e da vontade, possibilitando a transformação do poder comunicativo em poder administrativo (HABERMAS, 2004).

Na Teoria Crítica reconstrutiva de Habermas, não há espaço para uma divisão de trabalho excludente e exclusivista entre filosofia e ciências. A filosofia é despojada de sua função jurisdicional para atuar como colaboradora das diversas ciências na reconstrução dos conhecimentos científicos. Além disso, ela deve necessariamente se posicionar como uma intérprete-mediadora entre o mundo da vida e a cultura dos especialistas. Embora reconheça a ocorrência e as consequências da fragmentação da razão na modernidade, Habermas se distancia completamente da crítica negativista da razão promovida pelos teóricos da Escola de Frankfurt. Ele explica que o processo de modernização das sociedades industriais, caracterizado

por um sujeito com uma razão monológica, favoreceu a racionalidade cognitivo-instrumental. Habermas argumenta que o conceito de razão deve ser amplamente entendido para incluir seu aspecto dialógico.

Na modernidade, a razão substantiva da tradição pré-moderna foi dividida em três diferentes instâncias. Desde então, sua unidade assumiu um caráter meramente procedimental. Este caráter tripartido da razão foi teoricamente fundamentado nas três críticas de Kant (Crítica da Razão Pura, Crítica da Razão Prática e Crítica do Juízo), que se referem à racionalidade científica, ética e estética. Posteriormente, isso foi refletido nas formulações do jovem Hegel em Jena, que tripartiu a dialética em trabalho, interação e representação simbólica, e, na esfera sociológica, por Weber, que concebeu três distintos campos axiológicos: ciência, moral e arte. A interseção entre o direito e a sociedade da informação constitui um campo dinâmico e complexo, onde as normas jurídicas enfrentam o desafio de se adaptar às rápidas transformações tecnológicas e sociais.

Na Sociedade da Informação, o direito desempenha um papel crucial na regulamentação das tecnologias emergentes e na proteção dos direitos dos cidadãos. À medida que a tecnologia avança, a legislação enfrenta a pressão de se atualizar para refletir as novas formas de interação e transação digital. Algumas das transformações jurídicas mais significativas incluem: regulamentação da internet, proteção de dados e privacidade e propriedade intelectual. Os direitos digitais emergem como uma extensão dos direitos humanos tradicionais, adaptados ao contexto digital. Eles garantem que os indivíduos possam exercer seus direitos fundamentais na era da informação. Entre os principais direitos digitais, destacam-se: direito à privacidade, direito à liberdade de expressão, direito ao acesso à informação, direito à segurança cibernética.

O diálogo entre direito e tecnologia na sociedade da informação apresenta tanto desafios quanto oportunidades. Entre os desafios, está a necessidade de criar um marco regulatório que acompanhe o ritmo acelerado das inovações tecnológicas, sem sufocar a inovação. Por outro lado, há oportunidades para o desenvolvimento de novas áreas do direito, como a governança da inteligência artificial e a ética digital, que podem promover uma sociedade mais justa e equitativa. Análise Crítica das Estruturas de Poder também são relevantes: desigualdade de acesso, infraestrutura, alfabetização digital, impacto socioeconômico, vigilância governamental, poder corporativo e manipulação de informação.

Na moderna Sociedade da Informação, a Teoria Crítica do Direito sugere que o direito pode ser uma ferramenta para desafiar e redistribuir estruturas de poder na sociedade da informação. Nesse sentido, desenvolver leis que protejam os direitos digitais, garantindo que todos os indivíduos tenham acesso igualitário à tecnologia e proteção contra abusos de poder. Também, exigir que governos e corporações sejam transparentes em suas práticas de coleta e uso de dados, estabelecendo mecanismos de responsabilização para prevenir abusos. Cabe também promover o empoderamento comunitário, promovendo iniciativas que capacitem comunidades marginalizadas a desenvolver suas próprias soluções tecnológicas, fortalecendo a autonomia local e a resiliência digital. As inovações tecnológicas também podem ajudar a moldar essa evolução. IA levanta questões complexas sobre responsabilidade, ética e direitos humanos. A teoria crítica pode questionar quem controla essas tecnologias e como elas podem ser reguladas para prevenir discriminação e abuso. Com o aumento da coleta e análise de dados, a teoria crítica pode ajudar a desenvolver estruturas legais que protejam a privacidade dos indivíduos e garantam que eles tenham controle sobre suas informações pessoais.

À medida que as ameaças cibernéticas aumentam, a teoria crítica pode influenciar a criação de políticas (cibersegurança) que protejam tanto a segurança digital quanto os direitos humanos, evitando medidas excessivas de vigilância. Na sociedade da informação, onde a tecnologia desempenha um papel central na definição das interações sociais, econômicas e políticas, o direito enfrenta a necessidade urgente de adaptação. As inovações tecnológicas, como a inteligência artificial, a coleta massiva de dados e a conectividade global, apresentam questões complexas que desafiam as normas jurídicas tradicionais. Portanto, a Teoria Crítica do Direito, ao contrário de uma abordagem puramente teórica, propõe uma prática mediada pela teoria que busca realizar a razão nas relações sociais, promovendo liberdade, autonomia e emancipação humana. Theodor Ludwig Wiesengrund Adorno e Max Horkheimer, ao cunharem a expressão "teoria crítica", propõem um conhecimento voltado para a ação, não para a pureza. Eles destacaram que a teoria crítica deve interagir com a teoria tradicional para exercer influência libertadora (ADORNO, HORKHEIMER, 2006, p. 24). Adorno, em "Dialética Negativa", critica a noção de liberdade e destaca a centralidade do direito na lógica capitalista, apontando como a igualdade formal esconde desigualdades. Habermas, por sua vez, propõe uma democracia deliberativa baseada na ética discursiva, onde o mundo da vida orienta o sistema, assegurando a reprodução material. Ele vê a razão moderna fragmentada, mas

argumenta que deve incluir um aspecto dialógico (ADORNO, 2009). Na sociedade da informação, o direito enfrenta o desafio de regulamentar tecnologias emergentes e proteger direitos digitais, destacando a necessidade de um marco regulatório que acompanhe a inovação sem sufocá-la. A teoria crítica sugere que o direito pode desafiar e redistribuir o poder, promovendo transparência e empoderamento comunitário. O avanço da inteligência artificial e a coleta de dados levantam questões sobre ética e privacidade, áreas onde a teoria crítica pode influenciar políticas de cibersegurança.

A Teoria Crítica do Direito não é apenas acadêmica, mas um chamado à ação para moldar o futuro jurídico, promovendo uma redistribuição justa do poder e dos recursos em um mundo interconectado, garantindo que o progresso tecnológico seja sinônimo de progresso social. Deste modo, concluímos que a Teoria Crítica do Direito, fundamentada nas ideias de pensadores como Marx, Horkheimer, Adorno e Habermas, propõem uma análise do direito como um reflexo das relações sociais e econômicas, frequentemente ocasional aos interesses dos grupos dominantes. Em um mundo digitalizado, essa teoria se mostra essencial para criticar e desafiar as estruturas de poder e dominação, promovendo a emancipação humana. Na obra "Teoria Crítica I: uma documentação", Horkheimer destaca a importância de uma abordagem que considera a interdependência entre teoria e prática, não apenas uma crítica ao status quo, mas a construção de um marco regulatório que assegure os direitos digitais e promova a igualdade (HORKHEIMER, 2020, p. 184-191). A teoria crítica se posiciona como um meio de enfrentamento às desigualdades exacerbadas pela tecnologia, defendendo a transparência e o empoderamento das comunidades, assim como a necessidade de uma adaptação do direito frente às rápidas transformações sociais e tecnológicas. As discussões acerca do tema não se esgotam com o avanço das IA´s, ao contrário se intensificam e demonstram a urgência da criação de legislações específicas que regulamentem a implementação de inteligência artificial e suas tecnologias. As discussões sobre o tema não se esgotam com o avanço das Ias. Ao contrário, elas se intensificam, evidenciando a necessidade urgente de criar legislações específicas que regulamentem a implementação da inteligência artificial.

CONCLUSÃO

A conclusão da pesquisa revela a relevância contemporânea da Teoria Crítica do Direito, que, fundamentada nas ideias de Karl Marx, Max Horkheimer, Theodor Adorno e Jürgen

Habermas, oferece uma perspectiva inovadora sobre o papel do direito nas dinâmicas sociais e econômicas. O trabalho argumenta que o direito não é um sistema neutro, mas sim um reflexo das relações de poder que muitas vezes servem aos interesses dos grupos dominantes, especialmente em um contexto digital.

A análise destacou a interdependência entre teoria e prática, propondo que a teoria crítica não apenas crítica ao status quo, mas também busca soluções para a emancipação humana e a justiça social. Diante das rápidas transformações tecnológicas, a teoria crítica se torna uma ferramenta vital para abordar questões como direitos digitais, privacidade e registro. Assim, o texto enfatiza a urgência de um marco regulatório que responda às novas realidades da sociedade da informação, garantindo a transparência e o empoderamento das comunidades marginalizadas.

A Teoria Crítica do Direito, portanto, não é meramente uma reflexão teórica, mas um chamado à ação, essencial para moldar um futuro jurídico que assegure o progresso social e tecnológico, desafiando estruturas de dominação e promovendo a igualdade em um mundo interconectado. A continuidade da discussão sobre essas questões é crucial, especialmente diante das crescentes implicações da inteligência artificial e de outras tecnologias emergentes.

REFERÊNCIAS

ADORNO, Theodor Ludwig Wiesengrund. **Dialética Negativa**. Tradução: Marcos Antonio Casanova. Rio de Janeiro: Jorge Zahar, 2009.

ADORNO, Theodor Ludwig Wiesengrund; HORKHEIMER, Max. **Dialética do esclarecimento: fragmentos filosóficos**. Tradução: Guido Antonio de Almeida. Rio de Janeiro: Zahar, 2006.

FREITAG, Bárbara. **A Teoria Crítica: ontem e hoje**. 5. ed. São Paulo: Brasiliense, 1994.

HABERMAS, Jürgen. **O discurso filosófico da modernidade**. Tradução: Luiz Sérgio Repa e Rodnei Nascimento. São Paulo: Martins Fontes, 2000.

HABERMAS, Jürgen. **Verdade e justificação: ensaios filosóficos**. Tradução: Milton Camargo Mota. 2. ed. São Paulo: Edições Loyola, 2004.

HORKHEIMER, Max. **A atual situação da filosofia social e das tarefas de um Instituto de Pesquisas Sociais**. São Paulo: Hucitec, 1999.

HORKHEIMER, Max. **Teoria crítica I: uma documentação**. Vol. 77. 1. ed. Tradução: Hilde Cohn. São Paulo: Perspectiva, 2020.

HORKHEIMER, Max. **Teoria tradicional e teoria crítica**. Tradução: Edgard Afonso Malagodi e Ronaldo Pereira Cunha. In: Pensadores. 1. ed. São Paulo: Abril Cultural, 1975.

MARX, Karl. Introdução. **Crítica da filosofia do direito de Hegel**. Tradução: Rubens Enderle e Leonardo de Deus. São Paulo: Boitempo, 1843.

7 Information Society and Law
FMU CENTRO UNIVERSITÁRIO

TREINAMENTO DE INTELIGÊNCIA ARTIFICIAL COM DADOS DE NAVEGAÇÃO EM REDES SOCIAIS: ABORDAGENS, IMPLICAÇÕES ÉTICAS E IMPACTO NA PRIVACIDADE DOS USUÁRIOS

ARTIFICIAL INTELLIGENCE TRAINING WITH SOCIAL MEDIA NAVIGATION DATA: APPROACHES, ETHICAL IMPLICATIONS AND IMPACT ON USER PRIVACY

Claudia Silva de Oliveira Camargo[1]

Resumo: Com o crescimento das redes sociais, as plataformas digitais adquiriram um volume inédito de dados gerados pelos usuários, incluindo textos, imagens, vídeos e interações sociais. Estes dados são frequentemente utilizados para o treinamento de modelos de Inteligência Artificial (IA), que podem aprender a partir de linguagem, comportamento e preferências humanas. Embora essa prática possibilite avanços significativos na personalização de conteúdo e moderação de redes, ela também levanta questões éticas, especialmente em relação à privacidade dos usuários e ao uso adequado de seus dados pessoais. Este artigo examina os métodos de coleta e tratamento de dados de redes sociais, os principais modelos e algoritmos aplicados e as implicações éticas associadas ao uso dessas informações. Conclui-se com uma análise sobre o impacto dessa prática na privacidade dos usuários e recomendações para uma abordagem mais ética e transparente.
Palavras-Chave: inteligência artificial; treinamento de IA; privacidade; redes sociais; dados de navegação.

Abstract: With the growth of social networks, digital platforms have acquired an unprecedented volume of data generated by users, including texts, images, videos and social interactions. This data is often used to train Artificial Intelligence (AI) models, which can learn from human language, behavior and preferences. Although this practice enables significant advances in content personalization and network moderation, it also raises ethical questions, especially in relation to users' privacy and the appropriate use of their personal data. This article examines the methods of collecting and processing social media data, the main models and algorithms applied, and the ethical implications associated with the use of this information. It concludes with an analysis of the impact of this practice on users' privacy and recommendations for a more ethical and transparent approach.
Keywords: artificial intelligence; AI training; privacy; social networks; navigation data.

INTRODUÇÃO

Com a ascensão das redes sociais, plataformas como Instagram, Meta (Facebook) e X (anteriormente Twitter) passaram a coletar e armazenar grandes volumes de dados, que refletem

[1] Graduanda em Direito pela FMU – SP.

as interações humanas em ambiente digital. Estes dados incluem postagens, curtidas, compartilhamentos e comentários, e oferecem um cenário vasto e diversificado para o treinamento de modelos de IA. Essa prática tem o potencial de gerar avanços tecnológicos em áreas como personalização de conteúdo, detecção de discurso de ódio, análise de sentimentos e recomendação de produtos. No entanto, o uso de postagens para treinamento de IA suscita uma série de questões éticas, sendo a privacidade dos usuários uma das mais prementes.

Este artigo busca aprofundar a análise dos métodos e práticas que envolvem o uso de postagens de redes sociais para o treinamento de modelos de IA, abordando as tecnologias envolvidas, as aplicações e os impactos na privacidade dos indivíduos.

DISCUSSÕES E RESULTADOS

Metodologia de Treinamento de IA com Dados de Redes Sociais

O treinamento de IA com dados provenientes de redes sociais exige etapas estruturadas e cuidadosas de coleta, processamento, anonimização e balanceamento dos dados. A seguir, destacam-se essas etapas e suas características:

Coleta de Dados

A coleta de dados de redes sociais pode ser realizada por meio de interfaces de programação de aplicações (APIs) oferecidas por algumas redes, como Twitter e Instagram utilizando:

- Filtro de tópicos e relevância: O uso de palavras-chave, hashtags e outras características de filtragem para assegurar que o conteúdo coletado seja relevante para os objetivos do treinamento.
- Frequência e volume de dados: Redes sociais produzem grande volume de dados diariamente, exigindo métodos de coleta que possam manejar e armazenar eficientemente essa massa de informações.

Pré-Processamento de Dados

Os dados de redes sociais são predominantemente não estruturados e apresentam alto nível de informalidade, o que exige processamento para remover ruídos e ajustar o conteúdo. Esse pré-processamento envolve:

- Limpeza e normalização: Remoção de ruídos, como URLs, emojis e dados irrelevantes.

- Tokenização e vetorização: Estruturação dos textos para que possam ser processados por modelos de linguagem natural, convertendo as palavras em vetores de números que representam semanticamente os termos.

Anonimização e Privacidade

Devido à natureza pública e pessoal das redes sociais, o processo de anonimização dos dados é fundamental para garantir a privacidade dos usuários. Técnicas comuns incluem:

- Remoção de identificadores pessoais: Remoção de nomes, localizações e outros dados que possam identificar o usuário diretamente.
- Generalização de dados: Técnicas que substituem informações específicas por categorias mais amplas, reduzindo o risco de identificação sem perder contexto para o treinamento da IA.

Balanceamento e Diversidade de Dados

Para evitar vieses, é necessário que o conjunto de dados represente uma variedade demográfica e cultural. Em redes sociais, onde há uma pluralidade de grupos, o balanceamento de dados ajuda a minimizar o risco de enviesamento nos modelos de IA.

Aplicações de Modelos de IA Treinados com Dados de Redes Sociais

Redes sociais têm sido utilizadas para o desenvolvimento de modelos de IA em várias aplicações, algumas das quais incluem:

Análise de Sentimentos e Previsão de Tendências

Modelos de IA treinados em redes sociais são amplamente utilizados para interpretar o sentimento do público em relação a determinados tópicos. Isso é especialmente útil para empresas que monitoram a percepção dos consumidores sobre produtos, marcas ou eventos.

Moderação e Segurança de Conteúdo

Redes como Meta e X utilizam IA para identificar e moderar conteúdos nocivos, incluindo discurso de ódio, conteúdo violento e desinformação. Modelos de IA analisam postagens em tempo real, removendo conteúdos que infrinjam as políticas da plataforma e promovendo um ambiente mais seguro.

Algoritmos de Recomendação e Personalização

Esses modelos são essenciais para o fornecimento de conteúdo personalizado aos usuários. Utilizando o histórico de interações e preferências de cada indivíduo, a IA recomenda postagens, páginas e até produtos, aumentando a retenção e o engajamento na plataforma.

Publicidade Direcionada e Monetização

Os dados coletados também são utilizados para aprimorar a segmentação de anúncios, permitindo que redes sociais direcionem anúncios mais alinhados ao perfil de interesses de cada usuário. Essa prática potencializa a eficácia dos anúncios e, por consequência, os lucros da plataforma. No entanto, para que essa segmentação ocorra, é necessário um uso intensivo dos dados dos usuários, o que gera preocupações sobre privacidade e direitos autorais.

A publicidade direcionada, é uma estratégia amplamente utilizada por plataformas digitais, como o Instagram, Facebook e X, e se baseia na coleta e análise de dados dos usuários para personalizar anúncios levantando uma série de preocupações sobre a privacidade dos usuários. A seguir, exploramos os principais aspectos dessa questão:

Coleta Excessiva de Dados

Para oferecer publicidade direcionada, as plataformas precisam coletar uma vasta quantidade de dados dos usuários. Isso inclui não apenas informações explícitas, como dados demográficos e interesses informados, mas também dados implícitos, que são inferidos a partir do comportamento online, como:

- Interações com postagens: Curtidas, comentários e compartilhamentos ajudam a identificar interesses específicos.
- Navegação na web: O rastreamento de páginas visitadas e tempo gasto em diferentes conteúdos revela padrões de consumo e preferências.
- Atividades fora da plataforma: Muitos anunciantes utilizam cookies e pixel tracking para monitorar o comportamento do usuário em outros sites, o que pode ser combinado com dados de redes sociais.

Essa coleta massiva pode ser vista como uma invasão à privacidade, especialmente quando os usuários não têm ciência clara sobre quais dados estão sendo coletados e como serão usados.

Consentimento e Transparência

A publicidade direcionada geralmente depende do consentimento do usuário para a coleta de dados. Contudo, muitos usuários não leem ou compreendem as políticas de privacidade e os termos de serviço, o que pode resultar em um consentimento informado inadequado.

- Falta de clareza: Os usuários podem não entender quais informações estão sendo coletadas, como estão sendo usadas e por que motivos. Isso gera uma falta de transparência que prejudica a confiança na plataforma.
- Consentimento implícito: Em alguns casos, o consentimento é considerado implícito, levando à coleta de dados sem uma autorização explícita. Essa prática pode ser controversa, especialmente quando os usuários não estão cientes de que estão optando por compartilhar suas informações.

Reidentificação e Risco de Exposição

Mesmo quando os dados são anonimizados, existe o risco de reidentificação. Isso pode ocorrer quando dados coletados de várias fontes são combinados, permitindo que anunciantes ou terceiros identifiquem indivíduos específicos.

- Rastreamento de atividades: Se um usuário interage com múltiplas plataformas que compartilham informações entre si, suas atividades podem ser traçadas de volta a ele, comprometendo sua privacidade.
- Vulnerabilidades de segurança: Dados coletados podem ser vulneráveis a vazamentos ou acessos não autorizados, expondo informações pessoais que os usuários prefeririam manter em sigilo.

Manipulação e Controle

A personalização dos anúncios pode levar a uma forma de manipulação comportamental. Quando os usuários são constantemente expostos a anúncios que refletem suas preferências, isso pode moldar suas decisões de compra e influenciar seu comportamento sem que eles estejam cientes.

- Criação de "câmaras de eco": Anúncios personalizados podem reforçar crenças e preferências existentes, limitando a exposição a novas ideias e produtos, o que pode resultar em uma visão distorcida da realidade.
- Impacto em decisões sensíveis: Isso é particularmente preocupante em áreas como política e saúde, onde a manipulação da informação pode influenciar decisões importantes.

Regulamentação e Proteção de Dados

Diante das preocupações sobre privacidade, diversas jurisdições implementaram regulamentações, como o GDPR na União Europeia e a LGPD no Brasil, que visam proteger os dados dos usuários.

- Direito à privacidade: Essas leis oferecem aos usuários maior controle sobre suas informações, permitindo que eles solicitem a exclusão de dados, revisem as informações que uma plataforma possui sobre eles e optem por não participar de atividades de rastreamento.
- Responsabilidade das empresas: As plataformas são obrigadas a garantir que as práticas de coleta e uso de dados sejam transparentes e respeitem as preferências dos usuários. O não cumprimento pode resultar em penalidades severas.

Desafios Éticos e Impacto na Privacidade

Embora as redes sociais ofereçam dados valiosos para o treinamento de IA, a utilização dessas informações levanta desafios éticos, especialmente no que se refere à privacidade e à conformidade com regulamentações de proteção de dados, como o GDPR e a LGPD.

Questões de Privacidade e Consentimento

A coleta de dados de redes sociais para IA frequentemente ocorre de forma indireta, sem que os usuários tenham ciência ou consintam explicitamente para o uso de seus dados para treinamento. Essa prática viola o direito à privacidade, compromete a transparência da plataforma com seus usuários.

Viés e Discriminação

Modelos de IA treinados com dados de redes sociais podem refletir vieses demográficos e culturais inerentes às interações nas plataformas, uma vez que certos grupos estão mais representados que outros. Isso pode gerar modelos com respostas enviesadas, especialmente em questões sociais e políticas, reforçando estereótipos e discriminações.

Uso de Dados para Vigilância e Controle

Os dados das redes sociais treinam modelos que podem ser utilizados para vigilância social e controle de comportamento, com riscos de invasão de privacidade, monitoramento sem consentimento e potencial manipulação de decisões de usuários.

Perspectivas para Mitigação de Riscos e Futuras Direções

Dado o potencial impacto negativo do uso de redes sociais para treinamento de IA sobre a privacidade, diversas abordagens podem ser adotadas para reduzir os riscos e assegurar um uso mais ético dos dados:

Adoção de Normas Transparentes e Consentimento Esclarecido

É necessário que as redes sociais adotem políticas de privacidade que esclareçam como os dados são utilizados e obtenham o consentimento dos usuários de forma explícita para o uso de informações pessoais no treinamento de IA.

Controle e Auditoria de Viés nos Modelos de IA

Modelos treinados com dados de redes sociais devem passar por auditorias para detecção e correção de vieses. Métodos de equalização de dados e controle de variáveis demográficas podem ser empregados para garantir maior imparcialidade e representatividade.

Regulação e Compliance com Regulamentações de Privacidade

A implementação de regulamentações como o GDPR e a LGPD torna-se fundamental, exigindo que as plataformas se adequem a um padrão de proteção de dados, respeitando os direitos dos usuários. As redes sociais devem cumprir rigorosamente as normas de proteção de dados, sujeitando-se a auditorias e sanções em caso de falhas.

CONCLUSÃO

O treinamento de IA a partir de dados de redes sociais oferece benefícios expressivos em termos de personalização de conteúdo, moderação e aprimoramento da experiência digital. No entanto, o uso de informações de usuários requer uma abordagem ética que respeite a privacidade e os direitos individuais. Questões como anonimização, vieses e compliance com regulamentações de proteção de dados são centrais para o desenvolvimento responsável desses modelos. À medida que a IA evolui, é imperativo que as plataformas adotem práticas transparentes e responsáveis, proporcionando uma experiência digital segura e respeitosa com os dados de seus usuários.

REFERÊNCIAS

CÉSAR, P. **Conheça as Etapas do Pré-Processamento de dados - DataGeeks**. Disponível em: https://www.datageeks.com.br/pre-processamento-de-dados/. Acesso em: 27 out. 2024.

DA CNN. **IA generativa: especialista explica à CNN como é o treinamento da ferramenta**. Disponível em: https://www.cnnbrasil.com.br/tecnologia/ia-generativa-especialista-explica-a-cnn-como-e-o-treinamento-da-ferramenta/. Acesso em: 27 out. 2024.

ETAIN. **LGPD Cookies: o guia completo | SUA IMPRENSA**. Disponível em: https://suaimprensa.com.br/blog/lgpd-cookies-o-guia-completo/. Acesso em: 27 out. 2024.

FOTOS. **Instagram e Facebook usam suas fotos e textos para treinar IA: por que a prática está sendo questionada?** Disponível em: https://g1.globo.com/tecnologia/noticia/2024/07/01/instagram-e-facebook-usam-suas-fotos-e-textos-para-treinar-ia-por-que-a-pratica-esta-sendo-questionada.ghtml. Acesso em: 27 out. 2024.

HTTPS://GBASTOS811.JUSBRASIL.COM.BR. **Proteção de dados nas redes sociais | Jusbrasil**. Disponível em: https://www.jusbrasil.com.br/artigos/protecao-de-dados-nas-redes-sociais/1810106087. Acesso em: 27 out. 2024.

LGPD: como lidar com a proteção de dados nas mídias sociais? | Becker Direito Empresarial. Disponível em: https://www.direitoempresarial.com.br/lgpd-como-lidar-com-a-protecao-de-dados-nas-midias-sociais. Acesso em: 27 out. 2024.

META. **Meta não pode usar dados de usuários de redes sociais para treinar IA - Migalhas**. Disponível em: https://www.migalhas.com.br/quentes/410502/meta-nao-pode-usar-dados-de-usuarios-de-redes-sociais-para-treinar-ia. Acesso em: 27 out. 2024.

O que é: Pré-Processamento De Dados. Disponível em: https://estatisticafacil.org/glossario/o-que-e-pre-processamento-de-dados-guia-completo/. Acesso em: 27 out. 2024.

VEJA. **Governo manda Meta interromper treinamento de IA com dados de usuários**. Disponível em: https://veja.abril.com.br/coluna/maquiavel/governo-manda-meta-interromper-treinamento-de-ia-com-dados-de-usuarios. Acesso em: 27 out. 2024.

7 Information Society and Law
FMU CENTRO UNIVERSITÁRIO

DISCRIMINAÇÃO E VIOLAÇÕES DE DIREITOS HUMANOS PELO ALGORITMO

DISCRIMINATION AND HUMAN RIGHTS VIOLATIONS BY THE ALGORITHM

Eduardo Tognetti[1]

Resumo: o texto aborda como o uso crescente de algoritmos de inteligência artificial em diversas áreas tem gerado preocupações em relação à discriminação e às violações de direitos humanos, especialmente contra grupos vulneráveis. A metodologia utilizada será a da revisão bibliográfica. Discute-se a ideia de que, ao invés de serem neutros, os algoritmos podem reproduzir preconceitos históricos, como racismo e sexismo, refletidos nas próprias bases de dados utilizados para treiná-los. Além disso, exemplifica a perpetuação das desigualdades estruturais por meio de sistemas automatizados em processos como vigilância policial e concessão de benefícios sociais, que afetam desproporcionalmente minorias raciais e classes sociais mais pobres. A solução proposta passa por uma maior transparência e responsabilidade na criação desses sistemas, juntamente com a inclusão de princípios de justiça social desde o seu desenvolvimento.
Palavras-chave: Inteligência artificial; discriminação; violação de direitos humanos.

Abstract
The text discusses how the increasing use of artificial intelligence (AI) algorithms in various fields has raised concerns about discrimination and human rights violations, particularly against vulnerable groups. It highlights that, rather than being neutral, algorithms often reproduce historical biases such as racism and sexism, inherent in the data used to train them. It further illustrates how automated systems perpetuate structural inequalities in processes like police surveillance and social welfare distribution, disproportionately affecting racial minorities and lower social classes. The proposed solution involves greater transparency and accountability in developing these systems, along with the incorporation of social justice principles from their inception.
Keywords: artificial inteligence; discrimination; human rights violations.

INTRODUÇÃO

Nos últimos anos, o uso de algoritmos de inteligência artificial (IA) tornou-se uma prática comum em diversas áreas, incluindo segurança pública, saúde, educação e, sobretudo,

[1] Professor do Centro Universitário das Faculdades Metropolitanas Unidas (desde 2016). Doutor (2015) e Mestre (2012) pela Universidade de São Paulo (USP), sob orientação da Profa. Titular Maria Sylvia Zanella Di Pietro. Especialista em Direito do Estado pela PUC-SP (2009) e em Direito da Economia e da Empresa pela FGV-RJ (1998). Formado em direito pela PUC-RJ (1995). Advogado aposentado do Banco do Brasil (desde 2024). Parecerista do escritório Tognetti Advocacia - Sociedade de Advogados.

no setor privado. Embora as promessas tecnológicas ofereçam eficiência, precisão e soluções para problemas complexos, o uso de algoritmos também tem gerado preocupações profundas, especialmente no que tange à discriminação e violações de direitos humanos. Como consequência, a sociedade se vê diante de um dilema: os avanços tecnológicos podem agravar desigualdades já existentes, reforçando o preconceito e o racismo? Estaríamos repetindo os mesmos erros de Cesar Lombroso?

O presente trabalho aborda algumas das formas pelas quais algoritmos têm sido utilizados de forma discriminatória, contribuindo para a exclusão social de grupos vulneráveis e violando direitos humanos fundamentais, como o direito à igualdade, à privacidade e à não discriminação. A análise é fundamentada na obra de diversos autores e estudos recentes, que discutem como esses sistemas, em vez de serem neutros, podem reproduzir e amplificar preconceitos.

1 O HOMEM DELINQUENTE DE CESAR LOMBROSO

O Homem Delinquente (LOMBROSO, 2001) é uma obra originalmente publicada em 1876 pelo médico e criminologista italiano Cesare Lombroso, considerado um dos pioneiros da criminologia moderna. Seu trabalho é profundamente influenciado pelas teorias do positivismo, que buscam explicações científicas para o comportamento humano, especialmente no campo da criminalidade. O autor parte da premissa de que certos indivíduos possuem predisposições inatas para o crime, ideias que foram controversas à época e que continuam a ser criticadas até os dias atuais.

Na Itália do século XIX, quando Lombroso começou a desenvolver suas pesquisas, a Europa passava por uma transformação científica e social, com o avanço das ciências naturais e o crescimento do interesse por disciplinas como a psiquiatria e a antropologia. Nesse ambiente, Lombroso desenvolveu sua teoria da "atavismo" criminal (LOMBROSO, 2001, p. 266), que sugere que certos criminosos têm traços físicos, ou "estigmas", que os diferenciam do homem comum, remetendo a um estágio primitivo do desenvolvimento humano.

Lombroso argumenta que alguns indivíduos possuem características biológicas que os tornam mais propensos ao comportamento criminoso. Segundo ele, esses traços podem ser identificados através de uma análise minuciosa do corpo, particularmente da cabeça e do rosto. Seu conceito de "atavismo" refere-se a uma suposta regressão evolutiva, em que certas pessoas

apresentariam traços físicos que pertencem a estágios anteriores da evolução humana. Lombroso acreditava que esses indivíduos "atavísticos" eram uma espécie de "homem primitivo" preso em corpos contemporâneos, e que sua natureza violenta e impulsiva os levava a comportamentos delinquentes.

Entre os estigmas físicos descritos por Lombroso, encontram-se características como: mandíbulas proeminentes, arcos superciliares pronunciados, testa recuada, orelhas grandes ou malformadas, nariz achatado, além de braços longos e desproporcionais ao corpo. Essas características, segundo ele, seriam indicativas de uma predisposição ao crime.

Embora o trabalho de Lombroso tenha contribuído para a discussão de que o crime não deveria ser visto apenas como uma questão moral ou de livre-arbítrio, mas como um fenômeno multifacetado que envolvia elementos científicos, a ideia de que o comportamento criminoso poderia ser explicado exclusivamente por fatores biológicos levou a uma estigmatização dos indivíduos com certas características físicas, além de abrir precedentes para gravíssimas práticas discriminatórias.

O grave erro de Lombroso, de generalizar o perfil do criminoso a partir de análises individuais, pode estar sendo repetido pelos mecanismos de inteligência artificial, especialmente os que aprendem em pesquisas de sites na própria Internet, sem a interferência direta de um ser humano, que seja capaz de avaliar o juízo feito pela ótica moral e ética, como veremos.

2 DISCRIMINAÇÃO ALGORÍTMICA: O MITO DA NEUTRALIDADE TECNOLÓGICA

A ideia de que os algoritmos são "neutros" é amplamente contestada. Embora os algoritmos sejam criados para processar dados de maneira objetiva, os próprios dados nos quais eles se baseiam podem conter vieses históricos e sociais, como graves preconceitos de ordem racial. Tal desvio é constatado pela professora catedrática da Universidade da Califórnia em Los Angeles (UCLA), Safiya Umoja Noble (2018), segundo a qual os algoritmos de busca, como o do Google, refletem as desigualdades raciais e de gênero presentes na sociedade.

A autora explica que os algoritmos de busca são estruturados para maximizar o lucro das empresas por meio da publicidade segmentada, o que significa que as identidades e comportamentos dos usuários são transformados em produtos para serem vendidos a

anunciantes. Nesse contexto, grupos marginalizados são particularmente vulneráveis a serem explorados.

Sua pesquisa mostra que, quando os usuários pesquisavam termos como "garotas negras", os resultados frequentemente vinculavam essas mulheres a conteúdo sexualizado. Isso não é uma coincidência. Ao contrário, evidencia como os algoritmos, projetados por seres humanos e treinados em conjuntos de dados tendenciosos, podem reforçar estereótipos prejudiciais.

Outro exemplo discutido no livro envolve o uso de algoritmos em processos decisórios automatizados, como em admissões universitárias, processos seletivos de empregos e vigilância policial. Noble cita estudos que mostram que os algoritmos utilizados nesses contextos frequentemente prejudicam pessoas de cor, reforçando práticas discriminatórias existentes. O racismo algorítmico nesses sistemas não é apenas uma questão de preconceito consciente, mas de estruturas institucionais que codificam e perpetuam essas desigualdades, como afirma a autora:

> [...]há um contexto social ausente nas plataformas de mídia digitais, e isso faz falta, particularmente para grupos marginalizados que são representado problematicamente de forma estereotipa ou pornográfica, para aqueles que são vítimas de bullying, ou para aqueles que são consistentemente vítimas de abuso (…) Os resultados das buscas refletem os valores e normas dos parceiros e dos anunciantes das empresas de busca comercial e frequentemente refletem nossas crenças mais baixas e aviltantes, porque essas ideias circulam tão livremente e com tanta frequência que não normalizadas e extremamente lucrativas. (…) A noção dominante sobre mecanismos de pesquisa misóginos ou racistas são simplesmente um espelho da coletividade. Resultados de pesquisas problemáticos não apenas parecem 'normais' mas também inescapáveis, mesmo que essas ideias tenham sido desmentidas completamente por estudiosos" (NOBLE, 2018, p. 55-56).

A situação se agrava diante do mito da neutralidade da Inteligência Artificial, como afirma Noble:

> O status de monopólio do Google, somado a suas práticas algorítmicas de enviesar informação em direção aos interesses do capital neoliberal e das elites socioeconômicas dos Estados Unidos, resultou em um conjunto de informação que alega ter credibilidade, mas é na verdade um reflexo de interesses publicitários. (NOBLE, 2018, p. 57).

A discriminação algorítmica é particularmente visível em sistemas de reconhecimento facial. Estudo conduzido por Buolamwini e Gebru (2018) demonstrou que sistemas de reconhecimento facial de grandes empresas de tecnologia, como IBM e Microsoft, apresentam taxas de erro muito maiores ao identificar pessoas negras em comparação com pessoas brancas, especialmente mulheres negras, como se observa:

> Using the dermatologist approved Fitzpatrick Skin Type classification system, we characterize the gender and skin type distribution of two facial analysis benchmarks, IJB-A and Adience. We find that these datasets are overwhelmingly composed of lighter-skinned subjects (79.6% for IJB-A and 86.2% for Adience) and introduce a new facial analysis dataset which is balanced by gender and skin type. We evaluate 3 commercial gender classification systems using our dataset and show that darker-skinned females are the most misclassified group (with error rates of up to 34.7%). The maximum error rate for lighter-skinned males is 0.8%. The substantial disparities in the accuracy of classifying darker females, lighter females, darker males, and lighter males in gender classification systems require urgent attention if commercial companies are to build genuinely fair, transparent and accountable facial analysis algorithms. (BUOLAMWINI; GEBRU, 2018, p. 1).

Esse viés coloca essas populações em maior risco de vigilância indevida e até prisões equivocadas, o que representa uma grave violação dos direitos humanos à privacidade e à não discriminação, reforçando o determinismo biológico de Lombroso.

3 O REFORÇO DAS DESIGUALDADES ESTRUTURAIS

Outra crítica comum aos algoritmos é a sua capacidade de reforçar desigualdades estruturais já existentes. Eubanks (2018) argumenta que as ferramentas de IA frequentemente são utilizadas para tomar decisões que afetam negativamente as populações mais vulneráveis, como a distribuição de benefícios sociais e a concessão de empréstimos bancários. A autora menciona que algoritmos usados em agências governamentais norte-americanas frequentemente rejeitam pedidos de assistência social ou determinam quais famílias são mais propensas a cometer fraudes, com base em padrões de dados enviesados.

Eubanks destaca três estudos de caso específicos para ilustrar como a automação impacta negativamente as pessoas marginalizadas. O primeiro em Indiana**.** A autora analisa a implementação de um sistema automatizado de elegibilidade para benefícios, que resultou na negação em massa de assistência a milhares de cidadãos. "The automation’s impacts were devastating for poor and working-class Hooriers. Between 2006 and 2008, the state of Indiana denied more than a million applications for food stamps, Medicaid, and cash benefits, a 54 percent increase compared to the three years prior to automation" (EUBANKS, 2018, p. 50). Esse sistema, conclui Eubanks, desconsidera as complexidades da vida dos mais pobres, tratando suas necessidades com frieza burocrática.

O segundo caso, ocorrido em Los Angeles, consiste no uso de ferramentas automatizadas de gestão de dados para lidar com a população sem-teto em Los Angeles. Em vez de abordar as causas estruturais da falta de moradia, o sistema de rastreamento é usado para

classificar as pessoas sem-teto com base em seu "merecimento", criando uma hierarquia de quem "merece" ajuda. Mais grave ainda é a sua utilização para criminalização dos sem-teto, como sugere a autora:

> Some suspect that all data is being held for other purposes entirely: to surveil and criminalize the unhoused. (…) (EUBANKS, 2018, p. 114).

> According to federal data standards, service providers may disclose protected personal informatio in HMIS to law enforcement 'in response to … an oral request for the purpose of identifying or locating a suspect, fugitive, material witness or mising person'. The information tha the LAPD can acess is limited to name, address, date and place of birth, social security number, and distinguishing physical characteristics. But there is no mandatory review or approval process for oral requests. There is no requirement that the information released be limited in scope or specifc to an ongoing case. There is no warrant process, no departmental oversight, no judge involved to make sure the request is constitucional (EUBANKS, 2018, p. 115).

No terceiro caso, da Pensilvânia, é feita uma análise do sistema de vigilância infantil, no qual algoritmos são utilizados para prever se uma criança corre o risco de abuso ou negligência. Ela critica esse sistema por penalizar desproporcionalmente as famílias pobres e negras, ao mesmo tempo em que falha em reconhecer os contextos complexos em que elas vivem. (EUBANKS, 2018, p. 127 e seg.).

Eubanks argumenta que os sistemas de automação fazem parte de uma tradição de "pobreza digital", onde as ferramentas tecnológicas são usadas para reforçar a desigualdade. O problema não é a tecnologia em si, mas sim a forma como ela é projetada e implementada, quase sempre visando os mais pobres com mais severidade do que os ricos:

> As long as this invisible code is running in the background while we build new automated decision-making tools, the resulting technologies will profile, police, and punish the poor. This doesn't require bad intentions on the part of disigners, data scientists, or program administrators. In only requires designing 'in neutral', ignoring the entirely predictable consequences of super-charging alredy unequal and discriminatory systems. The choise to design a system optimized for neutrality and objectivity is a choice to support the status quo. To build instead a world of justice and abundance, we will need to design for equity, on purpose, brick by brick and byte by byte (EUBANKS, 2018, p. 223).

A autora faz uma grave denúncia dessas ferramentas, que se baseiam em dados históricos que refletem preconceitos raciais e de classe, que inevitavelmente reproduzem esses padrões, tal como Lombroso o fez. Como resultado, comunidades já marginalizadas tornam-se ainda mais vulneráveis, sem acesso a recursos essenciais. Isso não só perpetua a exclusão, mas também exacerba as desigualdades sociais e econômicas, violando o direito fundamental à igualdade e à justiça social.

4 MONITORAMENTO E VIGILÂNCIA

Um aspecto crucial das discussões sobre a discriminação algorítmica é a questão da privacidade. O uso massivo de dados pessoais para alimentar algoritmos, especialmente em contextos como redes sociais e serviços financeiros, levanta preocupações significativas sobre como esses dados são coletados e utilizados. Shoshana Zuboff (2019), professora emérita da Harvard Business School, cunhou o termo "capitalismo de vigilância" para descrever a maneira como empresas de tecnologia monitoram, registram e exploram o comportamento dos usuários para fins comerciais. Segundo a autora, a exploração algorítmica dos dados coloca em risco o direito à privacidade, uma vez que as informações pessoais são coletadas e usadas sem o consentimento explícito dos indivíduos.

No estudo, o capitalismo de vigilância é definido como um sistema econômico que "reclama unilateralmente a experiência humana como matéria-prima gratuita para ser traduzida em dados comportamentais" (ZUBOFF, 2019, p. 9). Empresas como Google, Facebook e Amazon seriam pioneiras nesse modelo de negócio, que começou a tomar forma nos anos 2000, quando o Google descobriu que os dados de usuários podiam ser usados não apenas para melhorar seus serviços, mas também para prever e modificar o comportamento de consumidores. Esses "dados excedentes", segundo a autora, são a base sobre a qual o capitalismo de vigilância se sustenta, gerando um ciclo de coleta incessante de informações sobre todos os aspectos da vida humana.

Zuboff compara o capitalismo de vigilância com as formas anteriores de capitalismo, como o industrial, mas enfatiza que o primeiro é mais invasivo e perigoso. Enquanto o capitalismo industrial explorava o trabalho humano e recursos naturais, o capitalismo de vigilância explora o comportamento humano de maneiras sem precedentes, criando um novo tipo de mercado baseado no controle do futuro. Ela observa que “os capitalistas de vigilância reivindicam um domínio exclusivo sobre nossos dados comportamentais” (ZUBOFF, 2019, p. 12), destacando a unilateralidade desse processo, onde os usuários se tornam, muitas vezes, involuntariamente, parte de um ciclo de extração de dados.

Um dos conceitos centrais do livro é a "espiral de vigilância", na qual a coleta de dados se expande continuamente, ultrapassando fronteiras éticas e legais. A autora mostra como a exploração desses dados não é apenas passiva; ela envolve técnicas ativas para prever e, eventualmente, modificar o comportamento dos usuários. Ao discutir as práticas do Facebook,

ela menciona que a empresa busca "desenvolver mecanismos que podem não apenas prever, mas também influenciar o comportamento em direção a fins comerciais" (ZUBOFF, 2019, p. 134). Isto seria um passo crucial em direção ao que chama de "poder instrumental", onde empresas de tecnologia assumem um papel autoritário em nossas vidas, controlando não apenas o que fazemos, mas também o que pensamos e como agimos.

Zuboff explora como o capitalismo de vigilância impacta diversos aspectos da sociedade, desde a economia até a política. Ela argumenta que a estrutura desse novo sistema econômico cria uma assimetria de poder sem precedentes entre empresas de tecnologia e os cidadãos. Um exemplo claro é o papel que a coleta de dados desempenhou nas eleições políticas e na manipulação da opinião pública, como no caso do escândalo da Cambridge Analytica, que utilizou dados de milhões de usuários do Facebook para influenciar votações, como a eleição presidencial dos EUA em 2016 e o referendo do Brexit no Reino Unido. "Esses eventos mostraram como a tecnologia de vigilância pode ser instrumentalizada para distorcer o processo democrático" (ZUBOFF, 2019, p. 245).

Zuboff também examina a forma como o capitalismo de vigilância exacerba desigualdades. Ao coletar dados em massa, as grandes empresas de tecnologia detêm o poder de decidir quem pode acessar informações, quais anúncios são exibidos para determinados grupos e até mesmo quem tem acesso a serviços essenciais. Este tipo de discriminação algorítmica agrava as divisões sociais, ao passo que os mais vulneráveis são os mais explorados. Segundo Zuboff, "a segmentação de mercado baseada em dados pessoais perpetua preconceitos e desigualdades, à medida que grupos marginalizados são alvos mais frequentes de discriminação digital" (2019, p. 198).

A vigilância quando aplicada de maneira discriminatória, afeta desproporcionalmente certos grupos sociais. Em países como os Estados Unidos, por exemplo, dados sobre a movimentação e os comportamentos de comunidades negras e latinas são frequentemente utilizados para alimentar sistemas de monitoramento policial, exacerbando a violência policial e a criminalização dessas comunidades (O'NEIL, 2016).

O livro de O'Neil desafia a crença de que os algoritmos são imparciais. Ela afirma que, como esses modelos são criados por pessoas, eles refletem inevitavelmente os preconceitos e prioridades de seus criadores. Um exemplo claro é o uso de algoritmos de policiamento

preditivo, que muitas vezes direcionam a vigilância para bairros de baixa renda, perpetuando ciclos de criminalização, como segue:

> Reading police chief William Heim had to figure out how to get the same or better policing out of a smaller force. So in 2013 he invested in crime prediction software made by PredPol, a Big Data start-up based in Santa Cruz, California. The program processed historical crime data and calculated, hour by hour, where crimes were most likely to occur. The Reading policemen could view the program's conclusions as a series of squares, each one just the size of two football fields. If they spent more time patrolling these squares, there was a good chance they would discourage crime. (O'NEIL, 2016, p. 76-77).

Além de serem tendenciosos, esses algoritmos frequentemente operam sem transparência ou supervisão, acabando por atingir majoritariamente negros e hispânicos, que vivem em bairros de mais baixa renda, área tidas como de maior ocorrência de crimes, como segue:

> These nuisance crimes are endemic to many impoverished neighborhoods. In some places police call them antisocial behavior, or ASB. Unfortunately, including them in the model threatens to skew the analysis. Once the nuisance data flows into a predictive model, more police are drawn into those neighborhoods, where they're more likely to arrest more people. After all, even if their objective is to stop burglaries, murders, and rape, they're bound to have slow periods. It's the nature of patrolling. And if a patrolling cop sees a couple of kids who look no older than sixteen guzzling from a bottle in a brown bag, he stops them. These types of low-level crimes populate their models with more and more dots, and the models send the cops back to the same neighborhood.
>
> This creates a pernicious feedback loop. The policing itself spawns new data, which justifies more policing. And our prisons fill up with hundreds of thousands of people found guilty of victimless crimes. Most of them come from impoverished neighborhoods, and most are black or Hispanic. So even if a model is color blind, the result of it is anything but. In our largely segregated cities, geography is a highly effective proxy for race. (O'NEIL, 2016, p. 78).

Aqui o "atavismo" de Lombroso atinge uma dimensão geográfica, mas igualmente busca identificar a ocorrência de futuros delitos a partir da generalização de fatos relacionados à violência, sob uma suposta neutralidade.

5 TRANSPARÊNCIA E RESPONSABILIDADE: DESAFIOS ÉTICOS E JURÍDICOS

Uma das maiores barreiras à justiça em casos de discriminação algorítmica é a falta de transparência. Muitos dos algoritmos utilizados por empresas e governos são considerados "caixas-pretas", já que operam com pouca ou nenhuma supervisão pública (CASTELVECCHI, 2016). Sem acesso aos critérios e decisões dos algoritmos, é quase impossível para as pessoas afetadas contestarem as decisões tomadas por essas tecnologias.

Diante desse cenário, torna-se necessária a criação de regulamentos específicos que exijam transparência e auditorias regulares dos sistemas de IA. Além disso, é fundamental que haja responsabilização legal para os desenvolvedores e utilizadores desses sistemas, quando comprovado que eles resultam em discriminação e violação de direitos. A proteção dos direitos humanos, neste contexto, requer não apenas políticas técnicas, mas também jurídicas e éticas, que garantam que os algoritmos estejam alinhados com os princípios fundamentais da dignidade humana.

6 INICIATIVAS E POSSÍVEIS SOLUÇÕES

Diante dos riscos apresentados pelos algoritmos, várias iniciativas têm surgido com o intuito de mitigar os impactos negativos dessas tecnologias. Uma das soluções mais promissoras é a incorporação de princípios de justiça social e equidade na fase de desenvolvimento dos algoritmos. Neste contexto, Reuben Binns (2018) aborda como as teorias de justiça da filosofia política podem ajudar a conceituar a equidade no aprendizado de máquina. O autor parte da ideia de que o problema da discriminação algorítmica, ou seja, quando os modelos de aprendizado de máquina resultam em decisões que afetam desigualmente grupos protegidos, como aqueles definidos por raça, gênero ou religião. Ele observa que, se houver padrões de discriminação no mundo real, os algoritmos podem acabar replicando essas desigualdades. Isso levanta a necessidade de definir a equidade nos sistemas de aprendizado de máquina de uma forma que possa ser operacionalizada.

O autor aborda várias definições de justiça em aprendizado de máquina que têm sido propostas na literatura recente. Essas abordagens tentam medir se os grupos protegidos são tratados de maneira diferente em relação aos não protegidos. Essas medidas podem ser limitadas, pois muitas vezes falham em capturar nuances importantes. Diferentes métricas de justiça podem ser mutuamente exclusivas, exigindo escolhas difíceis por parte dos programadores, como segue:

> Ideally, a system might be expected to meet all of these intuitively plausible measures of fairness. But, somewhat problematically, certain measures turn out to be mathematically impossible to satisfy simultaneously except in rare and contrived circumstances Kleinberg et al. (2016), and therefore hard choices between fairness metrics must be made before the technical work of detecting and mitigating unfairness can proceed. (BINNS, 2018, p.2).

Binns faz uma conexão entre as discussões sobre justiça na filosofia política e as questões emergentes no AM. Ele argumenta que muitas definições de justiça usadas no AM

refletem debates filosóficos antigos, como as ideias de igualitarismo e meritocracia. Ele sugere que a filosofia política pode esclarecer os debates sobre a justiça nos sistemas automatizados, fornecendo uma base mais robusta para lidar com as diferentes concepções de equidade. Por exemplo, o igualitarismo, uma corrente que defende a igualdade de tratamento, tem implicações diretas no AM. Binns escreve: "Fairness as used in the fair machine learning community is best understood as a placeholder term for a variety of normative egalitarian considerations" (BINSS, 2018, p. 2). Isso significa que, na maioria das vezes, as discussões sobre justiça nos algoritmos são, na verdade, reflexos de debates sobre como reduzir desigualdades entre grupos.

CONCLUSÃO

A discriminação algorítmica representa um desafio urgente no campo dos direitos humanos, e sua resolução requer uma abordagem multidisciplinar que envolva tecnologia, direito, ética e políticas públicas. Enquanto algoritmos têm o potencial de contribuir para uma sociedade mais eficiente e inclusiva, sem a devida supervisão e regulamentação, eles correm o risco de perpetuar e ampliar as desigualdades sociais, incorrendo no mesmo erro de Lombroso. É imperativo que desenvolvedores, governos e a sociedade civil trabalhem juntos para criar sistemas que sejam justos e transparentes, garantindo que a tecnologia sirva aos interesses de todos os seres humanos, e não apenas de uma minoria privilegiada.

REFERÊNCIAS

BINNS, Reuben. Fairness in machine learning: lessons from political philosophy. In: **Proceedings of Machine Learning Research**, v. 81, p. 1-15, 2018. Disponível em: https://proceedings.mlr.press/v81/binns18a/binns18a.pdf. Acesso em 18 Out. 2024.

BUOLAMWINI, Joy; GEBRU, Timnit. Gender shades: intersectional accuracy disparities in commercial gender classification. **Proceedings of Machine Learning Research**, v. 81, p. 1-15, 2018. Disponível em https://proceedings.mlr.press/v81/buolamwini18a.html#:~:text=Related%20Material-,Download%20PDF,-Supplementary%20PDF. Acesso em 10 Out. 2024.

CASTELVECCHI, Davide. Can we open the black box of AI? **Nature**. v. 538, n. 7623, p. 20-23, 2016. Disponível em: https://www.nature.com/news/can-we-open-the-black-box-of-ai-1.20731 . Acesso em 10 Out. 2024.

CRAWFORD, Kate; CALO, Ryan. There is a blind spot in AI research. **Nature**, v. 538, n. 7625, p. 311-313, 2016. Disponível em: https://www.nature.com/articles/538311a . Acesso em 8 Out. 2024.

EUBANKS, Virginia. **Automating inequality**: how high-tech tools profile, police, and punish the poor. New York: St. Martin's Press, 2018. [Edição Kindle].

LOMBROSO, César. **O homem delinqüente**. Porto Alegre: Ricardo Lenz, 2001.

NOBLE, Safiya Umoja. **Algorithms of oppression**: how search engines reinforce racism. New York: NYU Press, 2018. [Kindle]

O'NEIL, Cathy. **Weapons of math destruction**: how big data increases inequality and threatens democracy. New York: Crown Publishing Group, 2016. Disponível em: https://edisciplinas.usp.br/pluginfile.php/7574239/mod_resource/content/1/%28FFLCH%29%20LIVRO%20Weapons%20of%20Math%20Destruction%20-%20Cathy%20ONeal.pdf. Acesso em 2 Mar. 2024.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira de poder. Rio de Janeiro: Intrínseca, 2020.

7 Information Society and Law
FMU CENTRO UNIVERSITÁRIO

AUTOMAÇÃO NO JUDICIÁRIO: POTENCIAIS RISCOS E O PAPEL DA INTELIGÊNCIA ARTIFICIAL

AUTOMATION IN THE JUDICIARY: POTENTIALS, RISKS, AND THE ROLE OF ARTIFICIAL INTELLIGENCE

Sofia Martins Rangel Garcia[1]

Resumo: O presente artigo tem como objetivo debater o uso atual e potencial dos sistemas Modelos de Linguagem de Alta Escala (Large Language Model) no contexto atual de austeridade do Estado e atendendo aos princípios de celeridade processual, eficiência e visando a redução de custos para a administração pública, e suas repercussões morais, éticas e legais no contexto pós-digital.
Palavras-Chave: Inteligência Artificial; Celeridade Processual; Direitos Trabalhistas; Precarização.

Abstract: This article aims to discuss the current and potential use of Large Language Model systems in the current context of State austerity, adhering to principles of procedural efficiency, expediency, and cost reduction for public administration, as well as their moral, ethical, and legal repercussions in the post-digital context.
Keywords: Artificial Intelligence; Procedural Efficiency; Expediency; Labor Rights; Job Precarization.

INTRODUÇÃO

Com o advento do século 21, o fim do bloco socialista, a vitória do Neoliberalismo em oposição ao Welfare State e às teorias Keynesianas ao Zeitgeist ocidental, e as revoluções trazidas pelas novas tecnologias da revolução pós-digital em curso, novas perspectivas sobre Austeridade, Eficiência e o uso dos métodos produtivos e tecnológicos foram estabelecidas com o objetivo de garantir um funcionamento da máquina do Estado que permita desonerar o contribuinte, permitindo a redução de custos e maior eficiência. Visão esta notavelmente percebida no cenário político atual com as discussões sobre o Arcabouço Fiscal e o antigo Teto de Gastos, sendo o presente resumo escrito em meio à debates sobre os cortes de gastos ligados ao Arcabouço Fiscal.

[1] Bacharelanda em Direito pelo Centro Universitário das Faculdades Metropolitanas Unidas – FMU.

Sendo essa a realidade fática, não cabe a juristas debater a validade ou não de tais práticas e projetos, mas apenas debater questões relacionadas à Jurisdição, Processo e a estrutura do Judiciário.

As novas tecnologias, notavelmente os Modelos de Linguagem de Alta Escala (Large Language Model ou LLM), denominados popularmente como Inteligência Artificial, redes neurais com alta quantidade de parâmetros (na escala de bilhões ou mais), treinados com grande quantidade de textos através de aprendizado de máquina não-supervisionado rapidamente se tornou um dos temas mais discutidos da atualidade e amplamente utilizado por todo o setor privado, chegando, de acordo com pesquisa da Forbes Advisor coletada entre Março e Abril de 2023, até 53% dos empresários participantes usam a IA para melhorar os processos produtivos, 51% usa para automação de procedimentos e 97% dos empresários afirmando que a IA terá um efeito positivo em suas operações e negócios.

Por outro lado, no Judiciário, este debate ainda é relativamente incipiente até pela sua própria natureza rígida como parte da Administração Direta, dependente do Judiciário e do CNJ.

Apesar disso, este debate está acontecendo, e na 2ª Sessão Extraordinária de 2024 do CNJ, presidida pelo Min. Luís Roberto Barroso como iniciativa do projeto Justiça 4.0 (de cooperação entre o CNJ e o Programa das Nações Unidas para o Desenvolvimento (PNUD) reconheceu aumento expressivo do número de projetos de uso de Inteligência Artificial no Judiciário Brasileiro em 2023, de até 26% em relação ao período de 2022, e em 62 órgãos em comparação os 53 do levantamento de 2022.

1 O PAPEL DA IA NA EFICIÊNCIA E CELERIDADE PROCESSUAL

A Inteligência Artificial – através dos Modelos de Linguagem de Alta Escala já deixou a esfera de ficção cientifica e da conjectura para se tornar realidade prática da vida contemporânea no capitalismo da presente década desde lançamento, em 2022, do Chat GPT 3.0 pela OpenAI e, logo após, o desenvolvimento e popularização de IAs de Chatbot como a Gemini (antiga Bard) da Google LLC, ErnieBot da Baidu, Llama da Meta Platforms Inc e as IAs de produção de imagens como Stable Diffusion da Stability AI, Midjourney da Midjourney Inc, ou Dall-E da OpenAI.

A adoção dessa tecnologia, consequentemente, se tornou imperativo para a produtividade de qualquer organização pública ou privada, sendo amplamente utilizada por

grandes empresas privadas, é objeto de pesquisa sobre seu eventual uso nos judiciários nacionais em particular em relação ao seu potencial de celeridade e economia por (Zelenikow, 2017; Langbroek, 2019).

Sua adoção tem se tornado comum por Judiciários de diversos países do mundo, notavelmente na República Federal da Alemanha, que desde de 2022 tornou obrigatório o peticionamento eletrônico em processos e de arquivos da administração pública e burocráticos e extrajudiciais para a sua utilização em sistemas que utilizam IA com Compreensão Natural de Língua (Natural Language Understanding ou NLU) como o OLGA da IBM, que está sendo utilizado para a categorização de processos e documentos para garantir maior eficiência e celeridade para o judiciário, ou o FRAUKE (Frankfurt Judgement Configurator Electronic), utilizado para padronizar julgamentos de natureza consumerista relacionados à processos ligados ao setor das empresas de aviação civil.

No judiciário pátrio, tradicionalmente moroso, é debatido o uso da Inteligência Artificial a alguns anos, como no artigo de Weslei Gomes de Sousa, 2020 e aponta o mesmo potencial enorme de economia orçamentária anual e de maior celeridade no tratamento dos processos inclusive através do seu uso na categorização de documentos, arquivos, processos e padronização de julgados e menor tempo de tramitação entre áreas internas do órgão.

Como exemplo de sucesso e pioneirismo no Brasil, podemos citar o Projeto VictórIA, criado à partir uma parceria entre o STF e a UnB e derivado dos projetos Victor e RAFA2030, voltado para o tratamento conjunto de termas repetidos ou similar, permitiria enorme economia com questões de categorização e logística no tratamento da enorme quantidade de processos que precisariam ser analisados. Isso permitirá a substituição pelo trabalho humano por um sistema mais eficiente automatizar a separação de Recursos Extraordinários por Tema de Repercussão Geral.

2 VIÉS E LIMITAÇÕES DOS ALGORITMOS

Notoriamente, o uso da IA sofre de diversos obstáculos claros, uma vez que existe enorme diversidade de padrões lógicos, escolhas gramaticais escrita contextualizada e abordagens pessoais pelos juízes, desembargadores e operadores do direito no Judiciário que pode prejudicar a identificação de padrões e também gerar imprecisões, especialmente ao considerar que IAs contemporâneas não são de fato inteligentes mas uma simulação baseada

em aprendizado através de enorme amostra de textos e documentos. Tal evento que gera um outro desafio, que é a necessidade de retreinar as LLM cada vez que há alteração na lei (Langbroek, 2019).

Todos esses fatores contribuem para que soluções baseadas no uso de IAs produzam resultados imprecisos à medida que a complexidade da questão legal aumenta (Rosenthal & Yoon, 2011)

Já outros autores (J. LAI, J. WU, W. GAN E Z. QI, Large Language Models in Law: A Survey, 2023 p. 11 à 16) por outro lado, demonstram que grande parte dos desafios relacionados ao uso de LLMs, descrito no artigo como (i) defeitos em sets de dados, (ii) qualidade e padronização inadequada, (iii) interpretação imprecisa de conceitos jurídicos e legais, (iv) insegurança jurídica devido a disparidade em interpretações pelos modelos, também mencionando (v) desafios de ética, viés e justiça e a dificuldade dos sistemas de interpretar textos extensos e individualizar decisões, desafios que podem ser sanados nos anos futuros através do desenvolvimento e aprimoração dos LLMs existentes, incluindo o próprio ChatGPT da OpenAI, e através de melhor qualidade de dados e proteção à privacidade, melhorias na capacidade de processamento de textos longos, melhor adaptabilidade e inteligência e uma estrutura ética com mecanismos regulatórios.

Um dos enormes desafios é relacionado ao viés não-intencional que pode ser transmitido para a IA derivado de preconceitos individuais e estruturais que ferem a ética e o princípio da impessoalidade e da não-discriminação como por exemplo o racismo, o preconceito de gênero e classe e étnico dos julgadores, juristas e da amostra de textos usada para o treinamento da IA.

Estudos e pesquisas sobre decisões consideradas racistas e viés ligado ao dialeto vernacular em do réu em julgamentos criminais foi notado por V. Hofmann, P. R. Kalluri e D. Jurafsky et al (2024) prejudicando os julgados onde o réu era um cidadão americano que utilizava o dialeto African American Vernacular English associado com a população afro-estadunidense historicamente oprimida.

Mesmo na geração de imagens, o uso da IA demonstrou repetidamente um viés sexista e racista, sendo claro isso em artigo publicado na Nature por Ananya, 2024.

Também é de suma importância citar o desafio presente no estudo das LLMs do fenômeno denominado “caixa preta” em que a IA se comporta de forma imprevisível e

aparentemente autônoma, descrito desde 1991 por Dean Pomerleau durante pesquisa sobre ALVINN (Autonomous Land Vehicle in a Neural Network) – apesar do autor não ter cunhado esse termo – a Caixa Preta se tornou um fenômeno comum em LLMs, e mesmo se benéfico para o objetivo original do projeto, como é o caso da pesquisa sobre ALVINNs, em alguns casos que tratam especificamente de indivíduos com repercussões legais e sociais profundas e que requerem transparência e impessoalidade, seja no Judiciário ou no setor privado, esse fenômeno pode representar um enorme risco principalmente se analisado à luz dos vieses que a amostragem utilizada para o aprendizado neural pode gerar.

Por último, é claro que o papel humano no julgamento é de extrema importância para o Judiciário, e isso traz um extenso debate sobre a ética e os riscos da automação e substituição do trabalho humano por Modelos de Linguagem baseados em redes neurais.

3 IMPLICAÇÕES IDEOLÓGICAS E POLÍTICAS

Em atenção à incidência dessas novas tecnologias e a mudanças na estrutura do Judiciário e seu uso para um objetivo político claro, é importante que seja claro que o uso de tais ferramentas poderá fazer surtir efeitos por diversas ramificações da sociedade.

Se por um lado estamos falando da economia orçamentária, almejada no cenário político brasileiro tanto pelo atual governo Lula 3 quanto pelo prévio governo Bolsonaro, que poderá permitir melhor uso do dinheiro arrecadado, isso também implica na substituição da mão de obra, incluindo profissionais do direito e funcionários e servidores públicos, por algoritmos que não são capazes de participar da economia, de consumir, investir, comprar.

Essa tendência não é só um problema ao discutir a Administração Pública, mas também é uma questão amplamente debatida no futuro do próprio setor privado graças à automação e substituição da mão de obra humana por algoritmos e LLMs, situação que pode perpetuar e aumentar desigualdades sociais e a parcela desempregada da força de trabalho, o que, historicamente e inclusive no conceito marxiano de Exército Industrial de Reserva, é atrelado a maior desigualdade social referente a relação trabalhador-empresário e consequentemente, instabilidade social e econômica e queda e estagnação de salários e riscos à garantia de direitos trabalhistas.

Podemos citar como prólogo dos possíveis e eventuais conflitos trabalhistas e sociais a própria Greve do Sindicato dos Roteiristas de 2023 (2023 Writers Guild of America strike),

amplamente apoiada por sindicatos de roteiristas do Reino Unido, Austrália, Canadá, Israel, Irlanda, Suécia, Itália e França, que foi motivada pelo crescente uso de LLMs para a geração e automatização do trabalho criativo de roteirista. Uma das demandas da greve, inclusive, foi limitar a forma e jeito como os estúdios deverão usar Inteligências Artificiais.

De acordo com, J. Chen, X. Zhu, C. Yang, T. Feng et al 2024, há enorme espaço para aprimorar ainda mais a geração de conteúdo criativo através do uso de Inteligência Artificial inclusive no trabalho de produção de textos literários. Alowais, S.A., Alghamdi, S.S., Alsuhebany, N. et al., 2023 também demonstraram o uso de Inteligência Artificial para o ramo da medicina e seus potenciais resultados positivos e riscos.

Essas repercussões, por último, foram estudadas por Rebecca Kunkel, 2022, que discute as repercussões do uso dessa tecnologia para toda a profissão jurídica como um todo, o que ela define como "proletarização da profissão jurídica" com a perda da autonomia e valorização e um novo caráter operário na profissão jurídica.

É necessário que, ao debater essa questão de automação, também pensemos nas ramificações do uso de algoritmos que, demonstravelmente, não são "neutros", mas carregam vieses por si sós, e como talvez isso possa reforçar e replicar numa visão tecnocrática e liberal da construção da ideologia do Estado como uma máquina produtiva, ignorando o aspecto de agente protetor dos direitos sociais e o atendimento justo e humanitário dos cidadãos que tutela.

O uso de IA traz, portanto, um dilema importante a ser debatido sobre uma contradição entre eficiência e economia e uma desumanização do processo judicial, conforme Zelenikow (2017) e Langbroek (2019).

CONCLUSÃO

Conforme demonstrado pelo texto e pelas referencias citadas, a Inteligência Artificial tem um enorme potencial de melhorias para a sociedade, trazendo melhor uso do dinheiro público, maior eficiência, proporcionando melhor uso do trabalho humano e diminuindo custas e despesas.

Ao mesmo tempo, ela apresenta vários riscos potenciais e presentes que podem acarretar, em maior instabilidade social e política, conflitos trabalhistas, desigualdade social e a precarização do trabalho humano.

Dentro do Judiciário, maior aprimoramento da celeridade é algo não só almejado a décadas, como a morosidade é um problema amplamente reconhecido no judiciário mundial conforme Erica Bosio, 2023. O Judiciário eficiente também é reconhecidamente um dos motores do desenvolvimento econômico e da produtividade comercial, conforme Hobbes (1651), Max Weber (1905) e Adam Smith (1755).

A possibilidade de um judiciário mais eficiente, que se adeque as demandas da sociedade pós-digital em que vivemos, é algo que pode acarretar diversos benefícios para o interesse social e coletivo e ao Estado. Porém, o Judiciário jamais deve sacrificar seus compromissos com a imparcialidade, com a proteção dos direitos humanos em todas suas gerações e a justiça social.

É necessário, portanto, que esse equilíbrio seja conscientemente organizado através de robusta regulamentação visando impor transparência no uso desses algoritmos, evitando que o Judiciário se torne excessivamente tecnocrático e impessoal, com indispensável supervisão humana, instâncias regulatórias, mitigando vieses e trazer, futuramente, uma perspectiva de sistemas de IA auditáveis e abertos ao escrutínio público.

A participação de especialistas multidisciplinares e principalmente operadores do direito e juristas para ajustar os sistemas e garantir que decisões e processos controlados por IA não ferem direitos e garantias, considerando aspectos técnicos, éticos e sociais também é imperativo.

Em conclusão, considerando todas essas perspectivas, é crucial um marco regulatório específico que defina limites e formas para o uso da IA no judiciário, estabelecendo diretrizes para reforçar a integridade, ética e o compromisso social da Justiça.

REFERÊNCIAS

ANANYA. AI image generators often give racist and sexist results: can they be fixed? **Nature**, v. 627, n. 8005, p. 722-725, mar. 2024. DOI: 10.1038/d41586-024-00674-9. PMID: 38503880.

BOSIO, Erica. WORLD BANK GROUP. A Survey of Judicial Effectiveness. **Policy Working Paper 10501**, 2023. Disponível em: https://documents1.worldbank.org/curated/en/099330206262335739/pdf/IDU0c20eb45a08f4504cee09199072bada1c4771.pdf. Acesso em: 25 out. 2024.

BRASIL. Conselho Nacional de Justiça. **Justiça em Números 2022**. Brasília: CNJ, 2022. 332 p. Disponível em: https://www.cnj.jus.br/wp-content/uploads/2022/09/justica-em-numeros-2022-1.pdf. Acesso em: 25 out. 2024.

CHEN, Jing; ZHU, Xinyu; YANG, Cheng; SHI, Chufan; XI, Yadong; ZHANG, Yuxiang; WANG, Junjie; PU, Jiashu; FENG, Tian; YANG, Yujiu; ZHANG, Rongsheng. HoLLMwood: unleashing the creativity of large language models in screenwriting via role playing. **Findings Of The Association For Computational Linguistics: EMNLP 2024**. Miami, Florida, EUA, 2024. p. 8075-8121. DOI: arXiv:2406.11683. Association for Computational Linguistics.

DIÁRIO FEDERAL DA REPÚBLICA FEDERAL ALEMÃ. **Gesetzzur Einführung der elektronischen Akte in der Justizund zur weiteren Förderung des elektronischen Rechtsverkehrs**. 12 jul. 2017. Disponível em: https://www.bgbl.de/xaver/bgbl/start.xav?start=%2F%2F*%5B%40attr_id%3D%27bgbl117s2208.pdf%27%5D#bgbl%2F%2F*%5B%40attr_id%3D%27bgbl117s2208.pdf%27%5D__1730389187458. Acesso em: 25 out. 2024.

GOLDBART, Max. **Deadline**. UK Writers Guild Expresses Solidarity With WGA & Tells Members Not To Work On U.S. Projects For Strike Duration. 2 maio 2023. Disponível em: https://web.archive.org/web/20230502164534/https://deadline.com/2023/05/writers-guild-uk-wggb-solidarity-ban-non-members-1235353404/. Acesso em: 25 out. 2024.

HAAN, Katherine, **Forbes Advisor**. How Businesses Are Using Artificial Intelligence In 2024. 2024. Disponível em: https://www.forbes.com/advisor/business/software/ai-in-business/. Acesso em: 25 out. 2024.

HOBBES, Thomas. **Leviathan**. Capítulo XIII, 1651.

HOFMANN, V.; KALLURI, P.R.; JURAFSKY, D. AI generates covertly racist decisions about people based on their dialect. **Nature**, v. 633, p. 147–154, 2024. DOI: 10.1038/s41586-024-07856-5.

KUNKEL, Rebecca. Artificial Intelligence, Automation, And Proletarianization of The Legal Profession. **Rutgers Law School Legal Studies Research Paper Series**, 2023. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4387638. Acesso em: 25 out. 2024.

LANGBROEK, Philip. **International Journal for Court Administration**, 2019. Disponível em: https://iacajournal.org/articles/10.18352/ijca.292. Acesso em: 25 out. 2024.

LAI, Jinqi; GAN, Wensheng; WU, Jiyang. UNIVERSIDADE DE JINAN. **Large Language Models in Law: A Survey,** 2023. Disponível em: https://www.researchgate.net/publication/376310449_Large_Language_Models_in_Law_A_Survey. Acesso em: 25 out. 2024.

NTIM, Zac; GOLDBART, Max; WHITTOCK, Jesse; GOODFELLOW, Melanie. Australian & Canadian Guilds Tell Writers To Down Tools In U.S. As International Film & TV Unions React To WGA Strike. **Deadline**. 3 maio 2023. Disponível em:

https://web.archive.org/web/20230503164951/https://deadline.com/2023/05/writers-strike-international-unions-react-tv-and-film-1235353628/. Acesso em: 25 out. 2024.

PAUL M. SWEEZY. **Four Lectures on Marxism**. New York: Monthly Review Press, 1981.

POMERLEAU, Dean. Robotics Institute. **Efficient Training of Artificial Neural Networks for Autonomous Navigation**. Carnegie Mellon University, 1991. Disponível em: https://www.ri.cmu.edu/pub_files/pub3/pomerleau_dean_1991_1/pomerleau_dean_1991_1.pdf. Acesso em: 25 out. 2024.

ROSENTHAL, Jeffrey S.; YOON, Albert H. **Cornell Law Review**. v. 96, n. 6, 2011. Disponível em: https://scholarship.law.cornell.edu/clr/vol96/iss6/11/. Acesso em: 25 out. 2024.

SCHINDLER, Eckard. Judicial systems are turning to AI to help manage its vast quantities of data and expedite case resolution. **IBM Blog**. Disponível em: https://www.ibm.com/blog/judicial-systems-are-turning-to-ai-to-help-manage-its-vast-quantities-of-data-and-expedite-case-resolution/. Acesso em: 25 out. 2024.

SOUSA, Weslei Gomes de. UNB. Programa de Pós-Graduação em Direito da Universidade de Brasília. **Inteligência artificial e celeridade processual no Judiciário: mito, realidade ou necessidade?** Disponível em: http://www.realp.unb.br/jspui/handle/10482/38772. Acesso em: 25 out. 2024.

ZELENIKOW, John. **International Journal for Court Administration**, 2017. Disponível em: https://iacajournal.org/articles/10.18352/ijca.223. Acesso em: 25 out. 2024.

7 Information Society and Law
FMU CENTRO UNIVERSITÁRIO

O CONTO DA IA: A VIOLÊNCIA DE GÊNERO ALGORÍTMICA E OS DIREITOS HUMANOS

THE TALE OF IA: ALGORITHMIC GENDER VIOLENCE AND HUMAN RIGHTS

Ellen Maria Rocha da Silva[1]

Resumo: Na obra distópica O Conto da Aia, de Margaret Atwood, é apresentada a República de Gilead, um regime teocrático instaurado após guerras e radioatividade. Com o novo ordenamento social, as mulheres são destituídas de seus direitos fundamentais, sendo-lhes vedado, inclusive, o direito à educação e à leitura. Elas são consideradas propriedade estatal, tendo como função exclusiva a procriação, uma vez que a infertilidade se tornou uma questão endêmica. Assim, as mulheres são reduzidas a meros instrumentos do Estado, sujeitas à coação, violência e privação de seus direitos, configurando-se um quadro de opressão extrema e institucionalizada. Esse cenário de dominação e subjugação das mulheres na República de Gilead retrata uma violação sistemática dos direitos humanos, evidenciando um regime que desrespeita princípios fundamentais de dignidade, igualdade e liberdade. Em paralelo, aludindo a um jogo de palavras, temos "O Conto da IA (Inteligência Artificial)", que demonstra como o ambiente virtual tornou-se inóspito para as mulheres em razão dos algoritmos que podem perpetuar ou agravar a discriminação e a violência de gênero. Assim, o objetivo deste estudo é analisar como a IA e os algoritmos intensificam a revitimização das mulheres no ambiente virtual, tensionando uma reflexão sobre o poder da tecnologia e o viés discriminatório de gênero, como ele retroalimenta a violação dos direitos humanos das mulheres, explorado em uma narrativa crítica. A metodologia utilizada incluiu a revisão de literatura, doutrina e análise de jurisprudência, a fim de abordar os direitos humanos das mulheres e suas implicações nas plataformas e na internet. Por fim, levando-nos à conclusão de que os algoritmos, quando programados ou aplicados sem considerações éticas e de gênero, podem agravar a violência de gênero contra as mulheres. É imperativo que o desenvolvimento tecnológico ocorra, mas pautado na preservação dos direitos humanos e na igualdade de gênero.
Palavras-Chave: Direitos humanos; Violência de Gênero; Algoritmo.

Abstract: Margaret Atwood's dystopian novel The Handmaid's Tale presents the Republic of Gilead, a theocratic regime established after wars and radioactivity. Under the new social order, women are stripped of their fundamental rights, including the right to education and reading. They are considered state property and their sole function is to procreate, since infertility has become an endemic issue. Thus, women are reduced to mere instruments of the state, subject to coercion, violence and deprivation of their rights, creating a picture of extreme and institutionalized oppression. This scenario of domination and subjugation of women in the

[1] Graduada em Investigação Forense e Perícia Criminal no Centro Universitário Leonardo da Vinci (Uniasselvi). Bacharelanda de Direito no Centro Universitário das Faculdades Metropolitanas Unidas (FMU). Pesquisadora do Núcleo de Pesquisa e Extensão sobre a Pena e Execução Penal na (USP) e Grupo de Pesquisa de Efetividade Jurídica Estatal (FMU). Estagiária da Defensoria Pública do Estado de São Paulo.

Republic of Gilead portrays a systematic violation of human rights, showing a regime that disregards fundamental principles of dignity, equality and freedom. In parallel, alluding to a play on words, we have "The Tale of AI (Artificial Intelligence)", which shows how the virtual environment has become inhospitable for women due to algorithms that can perpetuate or aggravate discrimination and gender violence. Thus, the aim of this study is to analyze how AI and algorithms intensify the re-victimization of women in the virtual environment, stressing a reflection on the power of technology and the discriminatory bias of gender, how it feeds back into the violation of women's human rights, explored in a critical narrative. The methodology used included a literature review, doctrine and analysis of case law, in order to address women's human rights and their implications on platforms and the internet. In the end, it led us to the conclusion that algorithms, when programmed or applied without ethical and gender considerations, can aggravate gender-based violence against women. It is imperative that technological development takes place, but guided by the preservation of human rights and gender equality.
Keywords: Human rights; Gender violence; Algorithm.

INTRODUÇÃO

A intersecção entre a violência de gênero e a IA (Inteligência Artificial) evidencia como o ambiente virtual reverbera padrões discriminatórios e misóginos, culminando em uma violência algorítmica que atenta contra os direitos humanos da mulher, tanto no espaço virtual quanto nas relações sociais. Partindo dessa premissa, a obra "O Conto da Aia" de Margaret Atwood explora de forma contundente essas dinâmicas, retratando um futuro distópico onde a subjugação das mulheres é exacerbada por sistemas opressivos, refletindo as consequências da desumanização e da objetificação que podem ser ampliadas por tecnologias emergentes.

Para a elaboração do trabalho a metodologia escolhida foi a revisão de literatura, pautando-se também em doutrinas cumulada de análise de jurisprudencial, para investigar o impacto da IA e dos algoritmos na revitimização das mulheres no ambiente virtual. Considerando que as mulheres já enfrentam violência estrutural na sociedade, incluindo discriminação, assédio e exclusão, a pesquisa analisa como as tecnologias digitais podem agravar essas formas de violência, perpetuando e ampliando os danos por meio dos algoritmos. A comparação crítica entre a distopia de O Conto da Aia e os efeitos reais da IA pretende gerar uma reflexão sobre a violação dos direitos humanos das mulheres na sociedade contemporânea.

Sob esse prisma, a violência algorítmica grassa como um fenômeno que não apenas reproduz, mas intensifica a opressão de gênero, evidenciando a necessidade de uma reflexão crítica sobre as implicações éticas e sociais da IA na vida das mulheres.

Nesse diapasão, a análise de Manuel Castells sobre a Sociedade em Rede é fundamental para compreender as relações de gênero contemporâneas. Castells argumenta que a tecnologia e a comunicação digital moldam novas formas de interação social, extraindo essa linha de pensamento compreende-se que vogaria tanto a emancipação quanto a opressão nas redes.

> A convergência da evolução social e das tecnologias da informação criou uma nova base material para o desempenho de atividades em toda a estrutura social [...] construída em redes, define os processos sociais predominantes, consequentemente dando forma à própria estrutura social. (CASTELLS, 1999, p. 567).

Castells (1999) alude que sociedade moderna, movida por uma visão higienista e potencializada pelas tecnologias, mídias e mercado exerce controle sobre o corpo feminino. Portanto, as redes sociais, *verbi gratia*, podem ser ferramentas de empoderamento, onde mulheres se organizam e mobilizam em prol de seus direitos. No entanto, ao mesmo tempo, essas plataformas são palco de violência algorítmica, onde a misoginia é amplificada por mecanismos de controle e vigilância.

> Redes são estruturas abertas, capazes de se expandir de forma ilimitada, integrando novos nós desde que consigam se comunicar dentro da rede, ou seja, desde que compartilhem os mesmos códigos de comunicação (por exemplo, valores ou critérios de desempenho). (CASTELLS, 1999, p. 566).

O pensamento de que um algoritmo seria isento de preconceitos é ilusório, a neutralidade algorítmica tenta minimizar o viés humano, mas os algoritmos ainda carregam os preconceitos dos seus criadores, sendo influenciados por decisões e raciocínios humanos, individuais ou hierárquicos.

> A questão da neutralidade algorítmica surge como uma possível solução para a redução do viés humano em decisões onde o pensamento das pessoas pode sofrer influências indesejadas. No entanto, modelos computacionais não são isentos de vieses, pois são construídos e desenvolvidos a partir do raciocínio e das decisões humanas, seja de forma individual, coletiva por parte de uma equipe, ou hierárquica, derivando de uma autoridade superior. (TASO et al., 2023, p. 2).

A sigla TFGBV refere-se a *Technology-Facilitated Gender-Based Violence, Abuse, and Harassment,* em uma tradução livre: Violência de Gênero, Abuso e Assédio Facilitados pela Tecnologia. É percebido que o uso da tecnologia é central em diversas formas de violência e assédio contra mulheres e meninas, englobando também aquelas que enfrentam múltiplas formas de marginalização, como as pertencentes a minorias raciais, mulheres LGBTQIA+, e aquelas com deficiência ou em desvantagem socioeconômica. (KHOO, 2021).

> Increasingly, there is recognition that these forms of violence may be facilitated by the use of technology, and that technology facilitates emerging forms of violence

> including, but not limited to, non-consensual sharing of intimate images, private communications, or personal data; image-based sexual abuse; online harassment and abuse; technologyfacilitated sexual abuse; use of diverse forms of technology for surveillance and stalking; and targeted hacking.[2] (University of Melbourne; United Nations Population Fund, 2023, p. 4).

A TFGBV seria um produto da violência massificada pela IA trazendo à tona um fenômeno que não apenas reproduz, mas intensifica a opressão em face das mulheres e garotas. Em uma pesquisa realizada por Alexandra Robinson, especialista em violência de gênero do Fundo de População das Nações Unidas (UNFPA), ela afirma que 85% das mulheres entrevistadas testemunharam violência contra outras mulheres online. Essa porcentagem varia de acordo com as regiões, todavia cerca de 90% de mulheres na América Latina e África e 98% no Oriente Médio foram alvo preconceito e discriminação online. (UNRIC, 2023).

Os dados revelam que 58% das jovens na faixa etária entre 15 e 25 anos, que são mais ativas nas redes sociais, já sofreram assédio online. A violência online transcende os limites da rede e se manifesta no mundo real com ferramentas de GPS e dispositivos inteligentes são utilizados para agredir as vítimas, permitindo que agressores as persigam e controlem, inclusive seus veículos e eletrodomésticos. Esses tipos de violência geralmente provêm de parceiros íntimos que têm acesso aos dispositivos e às senhas das vítimas. (UNRIC, 2023).

A agência da ONU afirma que as *Big Techs*[3] devem ser responsabilizadas pelos danos decorrentes da omissão em relação a materiais nocivos e ao uso inadequado da tecnologia, especialmente no que diz respeito à proteção das mulheres e das questões de gênero. Nesse sentido, a responsabilidade das plataformas digitais é crucial para a criação de um ambiente online seguro e saudável, que proteja as mulheres de abusos, assédio e discriminação, promovendo um espaço de interação respeitosa e construtiva. (UNRIC, 2023).

Depreende-se que, as plataformas facilitam abusos sexistas e violentos, sendo manipuladas por usuários para atingir esses fins. Sistemas de feedback criam ciclos que incentivam conteúdos cada vez mais o discurso de ódio. Campanhas coordenadas promovem conteúdo extremista, ocultam postagens feministas e marginalizadas, utilizam denúncias falsas

[2] Tradução livre: Reconhece-se cada vez mais que estas formas de violência podem ser facilitadas pela utilização da tecnologia e que esta facilita formas emergentes de violência, incluindo, entre outras, a partilha não consentida de imagens íntimas, comunicações privadas ou dados pessoais; o abuso sexual com base em imagens; o assédio e o abuso em linha; o abuso sexual facilitado pela tecnologia; a utilização de diversas formas de tecnologia para vigilância e perseguição; e a pirataria informática direcionada.
[3] Grandes empresas de tecnologia que predominam o mercado e atuam em áreas distintas, como Meta, Google, Amazon.

para banir ou silenciar essas vozes. Além disso, algoritmos amplificam conteúdos prejudiciais, como fotos íntimas ou informações pessoais resultantes de *doxing*. (KHOO, 2021).

> As for other platform affordances, there is no shortage of ways in which they facilitate sexist, misogynistic, and sexually violent abuse and harassment, or are exploited and gamed by users to achieve the same objectives. "Easy feedback systems… lead to discursive loops, in which influencers build audiences that ask for, or reward, certain types of content [...] algorithms assist in further disseminating this content, including intimate photos or personal information obtained through doxing, such as the person's home address.[4] (KHOO, 2021, p. 57).

Entre as práticas que infringem os direitos das mulheres através da tecnologia temos desinformação e difamação, assédio cibernético, discurso de ódio, falsificação de identidade, pirataria informática e perseguição, *astroturfing*, abuso baseado em vídeo e imagem, *doxxing*, ameaças violentas e imagens indesejadas ou conteúdos sexualmente explícitos. (UNRIC, 2024).

Com base na reportagem das Nações Unidas, que extraiu dados de uma pesquisa realizada pelo *The Economist*, da prevalência global de violência online contra a mulher, elaboramos uma tabela para facilitar a compreensão das informações.

Os tópicos foram separados em:

I – O tipo de violência;

II- O que significa cada uma delas;

III – O percentual geral por tática de ameaça à nível global.

[4] Tradução livre: Quanto às outras funcionalidades das plataformas, não faltam maneiras pelas quais elas facilitam abusos e assédios sexistas, misóginos e sexualmente violentos, ou são exploradas e manipuladas por usuários para alcançar os mesmos objetivos. "Sistemas de feedback simples… levam a ciclos discursivos, nos quais influenciadores constroem audiências que pedem ou recompensam certos tipos de conteúdo [...] os algoritmos ajudam a disseminar ainda mais esse conteúdo, incluindo fotos íntimas ou informações pessoais obtidas por doxing, como o endereço residencial da pessoa.

TIPO DE VIOLÊNCIA	O QUE SIGNIFICA?	%
Desinformação e difamação	Espalhar informação falsa ou prejudiciais sobre alguém	67%
Assédio cibernético	Assédio cibernético é a agressão repetida a alguém por meio digital, causando danos emocionais.	66%
Discurso de ódio	Expressões de ódio direcionados a indivíduos ou grupos	65%
Falsificação de identidade	Criação de perfis falsos para enganar os outros	63%
Pirataria informática e perseguição	Uso não autorizado de software, dados ou conteúdos digitais sem autorização para perseguir alguém	63%
Astroturfing	Compartilhar simultaneamente conteúdos prejudiciais em todas as plataformas	58%
Abuso baseado em vídeo e imagem	Uso indevido de vídeos ou imagens para abuso	57%
Doxxing	Divulgação de informações pessoais sem consentimento	55%
Ameaças violentas	Intimidação de alguém com a intenção de causar dano físico ou psicológico, realizada online.	52%
Imagens indesejadas ou conteúdos sexualmente explícitos	Envio de conteúdos sexualmente explícitos sem consentimento	43%

(Fonte: UNRIC, 2024)

Por derradeiro, cumpre esclarecer que o presente estudo tenciona realizar uma análise crítica da relação entre gênero e a IA em uma Sociedade em Rede, na qual o mundo online e real entrelaçam-se, caracterizando um “Conto da IA” que será explorado subsequentemente.

1 O GÊNERO E CASTIGO

No clássico russo Crime e Castigo, o protagonista *Raskólnikov* comete um crime e, ao longo da trama, enfrenta as consequências de seus atos, tanto psicológicas quanto sociais. Em síntese, fazendo uma analogia, o gênero carrega uma simbologia que impõe diversas consequências à mulher, as quais podem ser interpretadas como castigos sistematizados pelo patriarcado. Esse corolário é moldado pelas relações sociais que cercam a mulher, refletindo um sistema que a submete a normas e expectativas opressivas.

A corroborar com o exposto acima, Simone de Beauvoir (2019) preleciona que ser mulher é uma construção social e por isso "Não se nasce mulher, torna-se”. O peso cultural sobre o corpo ao nascer arraiga uma influência que moldará as experiências e expectativas do que é ser mulher, rotulando-a.

Ela argumenta que, historicamente, as mulheres sempre foram pressionadas a cumprir funções baseadas em seu gênero. Embora tivessem alguns direitos, os costumes prevaleciam, e o equilíbrio era mantido de tal forma que a mulher nunca alcançava uma liberdade plena.

Beauvoir (2019, p. 187) “Os direitos e os costumes nem sempre coincidiam: e, entre eles, o equilíbrio se estabelecia de maneira que a mulher nunca fosse concretamente livre”.

Outrossim, merece ser trazida à baila Judith Butler autora do livro Problemas de Gênero, para ela o gênero é pautado em uma construção social, logo não seria algo “natural” e sim uma “performance cultural” que é reproduzida por intermédio de práticas e discursos repetidos. Sendo assim, ele deveria ser descontruído por ser algo que não é compreendido, uma vez que ele é uma invenção, fomentado por ações e comportamentos reiterados que seguem normas sociais específicas.

> Ser mulher constituiria um “fato natural” ou uma performance cultural, ou seria a “naturalidade” constituída mediante atos performativos discursivamente compelidos, que produzem o corpo no interior das categorias de sexo e por meio delas? (BUTLER, 2020, p. 8).

Desde os primórdios da existência humana, a construção de papéis sociais tem regulado a conduta dos indivíduos, atribuindo funções conforme o gênero, com o intuito de instaurar harmonia e ordem na coletividade. Nesse cenário, o papel feminino na sociedade é objeto de amplas discussões e questionamentos, uma vez que a interação das mulheres com as instituições revela-se desvantajosa em comparação a dos homens. Um dos fatores que contribuem para essa desvalorização é o patriarcado, cujas origens remontam à Grécia Antiga e que persiste até os dias atuais.

Um exemplo representativo pode ser encontrado em um dos mais antigos códigos de leis, posterior ao Código de Hamurabi: o Código de Manu, que vigorou entre os séculos II a.C. e II d.C. Essa lei impunha uma desvalorização da mulher, estabelecendo que suas vontades não poderiam ser manifestadas e que sua conduta seria regulada por normas legais. O artigo 420 dispõe que: "Uma mulher está sob a guarda de seu pai durante a infância, sob a tutela de seu marido durante a juventude e sob a responsabilidade de seus filhos em sua velhice; ela não deve jamais conduzir-se à sua vontade."

Na transição entre a Idade Média e o Renascimento, a mulher era vista como um objeto doméstico e sexual, enquanto seus maridos estavam em guerra, ficando responsáveis pela educação dos filhos e sem autonomia. A obra de Gil Vicente, A Farsa de Inês Pereira, escrita em 1523, ilustra claramente o estereótipo muito associado à mulher: antes do casamento, ela ocupava-se com as tarefas domésticas, após a união, encontrava-se subordinada ao cônjuge. Na peça, a Inês, que deseja casar-se com um homem educado e de bons costumes para se libertar das obrigações do lar.

Entretanto, ela acaba se casando com Brás da Mata, um escudeiro, mesmo contra a vontade de sua mãe. Após o casamento, o seu marido impõe diversas regras, obrigando-a a permanecer reclusa, proibindo a Inês até de olhar pela janela ou frequentar a missa. Em uma passagem da obra, Brás da Mata justifica sua conduta afirmando que apenas protege sua mulher, o seu "tesouro", razão pela qual deseja "guardá-la" para si:

> INÊS: Que pecado foi o meu? Por que me dais tal prisão? ESCUDEIRO: Vós buscastes discrição, Que culpa vos tenho eu? Pode ser maior aviso, Maior discrição e siso Que guardar o meu tisouro? Não sois vós, mulher meu ouro? Que mal faço em guardar isso?" (VICENTE, 1523).

A ilustre Nísia Floresta Augusta, nascida em 12 de outubro de 1810, é reconhecida como uma das precursoras do feminismo. Como educadora, dedicou-se à promoção da educação das mulheres, à defesa dos direitos dos indígenas, à abolição da escravidão e à liberdade religiosa.

Em seu livro Direitos das Mulheres e Injustiça dos Homens, ela enfatiza a importância de lutar contra as desigualdades de gênero e questiona os paradigmas sociais que perpetuam a opressão das mulheres, defendendo a necessidade de uma transformação nos direitos e na posição social feminina.

> Se cada homem, em particular, fosse obrigado a declarar o que sente a respeito de nosso sexo, encontraríamos todos de acordo em dizer que nós nascemos para seu uso, que não somos próprias senão para procriar e nutrir nossos filhos na infância, reger uma casa, servir, obedecer e aprazer aos nossos amos, isto é, a eles homens." (FLORESTA, 1989, p.35).

No Brasil, no século XX, uma das punições que a mulher poderia receber por quebrar os paradigmas era ser embarcada no Trem dos Doidos, uma locomotiva que transportava os futuros internos do Hospital Colônia, em Barbacena, o maior hospício da época, conhecido como o Holocausto Brasileiro por tratar os pacientes de forma semelhante à que os nazistas fizeram com os prisioneiros na Segunda Guerra Mundial. Estima-se que 60 mil pessoas morreram nesse centro hospitalar.

> Cerca de 70% não tinham diagnóstico de doença mental. Eram epiléticos, alcoolistas, homossexuais, prostitutas, gente que se rebelava, gente que se tornara incômoda para alguém com mais poder. Eram meninas grávidas, violentadas por seus patrões, eram esposas confinadas para que o marido pudesse morar com a amante, eram filhas de fazendeiros as quais perderam a virgindade antes do casamento. Eram homens e mulheres que haviam extraviado seus documentos. Alguns eram apenas tímidos. (ARBEX, 2013, p. 13).

Como "pacientes", ainda que não tivessem nenhuma enfermidade mental, as mulheres sofriam diversas agressões físicas e psicológicas. Dentre elas o estupro, sessões de eletrochoque, lobotomia, passavam frio e fome. Todas que fizessem ou falassem algo não aceito

deveriam ser caladas, e o Hospital Colônia foi um lugar que a sociedade encontrou para silenciar as mulheres que perturbavam ordem e a moral.

No final do século XX, a mulher passou a ter maior reconhecimento com a promulgação da Constituição Federal de 1988, especificamente no art. 5º, que assegura a igualdade de direitos entre homens e mulheres. Essa foi uma conquista significativa, considerando que, até então, a simples ideia de que uma mulher pudesse ter a mesma importância que um homem era visto como um disparate. A mobilização e a pressão durante o processo constituinte por um grupo denominado de "Bancada do Batom" representado por 26 mulheres eleitas na em 1986 para a nova Assembleia Constituinte foi vital para essa transformação. (BRASIL, 2023).

> Cerca de 80% dessas propostas foram incorporados ao texto constitucional, assegurando às mulheres diversos direitos fundamentais, como a licença-maternidade de 120 dias, a proteção do mercado de trabalho e a proibição de diferença salarial, de exercício de funções e de critério de admissão. A nova Constituição também criou novas obrigações do Estado brasileiro de implementar políticas públicas voltadas para a salvaguarda das mulheres na sociedade. (BRASIL, 2023).

Malgrado, a igualdade esteja prevista em nossa Carta Magna, isso não significa que, de uma hora para outra, toda a sociedade passou a tratar a mulher de forma justa, deixando de lado os julgamentos e críticas formulados ao longo dos séculos.

> A evolução histórica da sociedade em considerar e até mesmo aceitar a ideia de que todos são merecedores de direitos humanos, sem sombra de dúvidas é um avanço de muitas gerações. Entretanto, assiste-se a falta de aplicabilidade dos direitos existentes, seja por violação de outro indivíduo ou até mesmo pelo próprio Estado, que supostamente deveria salvaguardá-los. (SILVA, 2023, p. 7).

No Brasil, o caso de Maria da Penha exemplifica essa problemática; após ser vítima de violência doméstica e sobreviver a duas tentativas de feminicídio, sua busca por justiça foi frustrada. Mesmo com a condenação de seu agressor, a liberdade dele durante o julgamento e a redução da pena destacam a falha do sistema em proteger os direitos das mulheres, levando-a a recorrer à Convenção Interamericana de Direitos Humanos.

> O Brasil é signatário da Convenção Americana dos Direitos Humanos de 1969 que foi ratificada em 1992, a qual é popularmente conhecida como Pacto de San José da Costa Rica. A Corte Interamericana condenou o Brasil e apontou violações nas garantias judiciais e proteção judicial, decidiu o pagamento de uma indenização a ela e recomendou que o estado tomasse medidas para eliminar a tolerância do estado em quaisquer tipos de violência doméstica. À vista do exposto, podemos dizer que graças ao Pacto de San José da Costa Rica tivemos um fortalecimento nos direitos humanos da mulher. (SILVA, 2023, p. 7).

Em 1993 a ONU adotou a Declaração Sobre a Eliminação de Violência Contra a mulher que estabelece a definição o que é a violência contra o gênero feminino, sendo ele "qualquer

ato de violência baseado no gênero que resulte, ou possa resultar, em dano físico, sexual ou psicológico ou em sofrimento para a mulher, inclusive as ameaças de tais atos, coerção ou privação arbitrária da liberdade, podendo ocorrer na esfera pública ou na esfera privada". (PIOVESAN, 2023).

Para Naomi Wolf, a dor é inerente à existência da mulher em função do mito da beleza, que é sustentado pelos estereótipos de gênero. Esse sofrimento, inobstante ser amplamente conhecido, não é levado a sério, nem mesmo no âmbito judiciário. A autora destaca que a dor feminina é tratada como um "ruído de fundo", ignorada e naturalizada. Isso resulta na legitimação da violência contra a mulher nas instituições, uma vez que ordenamento jurídico não reconhece essa dor, o que torna difícil para as mulheres provarem que foram vítimas.

> O que faz a dor existir? A jurista Suzanne Levit salienta que nos tribunais, para que se prove que algum mal foi feito, é preciso provar que se está em piores condições do que antes. Para ela, porém, como as mulheres estão cercadas por uma espécie de "ruído de fundo" que as agride, não se considera que elas estejam prejudicadas quando na verdade estão. (WOLF, 2020, p. 366).

1.1 A legislação e o desafio de proteger as mulheres frente às violências digitais

Em nosso ordenamento jurídico a perspectiva de gênero ainda é um desafio a ser enfrentado, é imprescindível termos uma nova visão no direito, sociedade e resto do mundo que traduza a urgência em reconhecer a mulher como um sujeito de direito. (PIOVESAN, 2011).

> Incorporar a perspectiva de gênero na doutrina jurídica brasileira impõe, sobretudo, o desafio de mudança de paradigmas. Esse desafio aponta a necessidade de introjetar novos valores e uma nova visão de Direito, de sociedade e de mundo. Traduz também a necessidade de inclusão de grande parcela da população mundial e da inclusão de seu modo de perceber e compreender a realidade. (PIOVESAN, 2023, p. 440).

O doutrinador Nucci (2023, p. 99) explica que:

> Culturalmente, em várias partes do mundo, a mulher é inferiorizada sob diversos prismas. Pior, quando é violentada e até mesmo morta, em razão de costumes, tradições ou regras questionáveis [...] No Brasil, verificou-se (e ainda se constata) uma subjugação da mulher no nível cultural, que resvala em costumes e tradições.

A Lei 11.340/2006 (Lei Maria da Penha) estabelece normas para proteger a condição da mulher, especialmente em relacionamentos domésticos. O feminicídio é uma extensão dessa proteção, caracterizando o homicídio de mulheres como uma qualificadora objetiva ligada ao gênero, conforme a lei supramencionada. Historicamente, o androcentrismo e a misoginia contribuíram para a opressão das mulheres, justificando a violência contra elas. (NUCCI, 2023).

No entanto, é de suma importância dizer que, recentemente, no dia 10/10/2024, foi sancionada a Lei 14.994/24, que transforma o feminicídio em um crime autônomo,

determinando como pena de 12 até 40 anos. O aumento da punição para o ato vil de ceifar a vida de uma mulher apenas por sua condição de gênero não é suficiente para evitar mais mortes.

Sublinha-se que o último anuário do Fórum de Segurança Pública expôs um crescimento de todas as formas de violência contra a mulher no ano de 2022. Vale salientar que a perseguição, também conhecida como *stalking*, resultou em 56.560 casos de mulheres vítimas em 2022. Ele é um alto fator de risco por ser um antecessor da ocorrência de feminicídios.

Para elucidar o que seria *stalking,* é um crime de perseguição incluído pela Lei n.º 14.132/2021 no código penal, sua definição, com fulcro no art. 147-A é "Perseguir alguém, reiteradamente e por qualquer meio, ameaçando-lhe a integridade física ou psicológica, restringindo-lhe a capacidade de locomoção ou, de qualquer forma, invadindo ou perturbando sua esfera de liberdade ou privacidade".

A referida prática também ocorre de forma digital, nessa vereda é explicado por McLachlan (2022, apud Fórum Brasileiro De Segurança Pública, 2023) "Mesmo a perseguição no mundo digital tem sido apontada como fator de risco para a violência letal contra mulher, indicando que a tecnologia facilita o controle e uma violência onipresente contra a mulher".

Destarte, as novas tecnologias possibilitam a sofisticação dos meios de aviltar a existências das mulheres. Em 2013, Brunna Rosa utilizou o termo "Feminicídio 2.0" para definir as novas formas de violência contra a mulher nas mídias sociais, facilitadas pelo uso da tecnologia.

> As mídias digitais (Internet: redes sociais, aplicativos, sites e afins) também podem ser utilizadas como instrumento para disseminar preconceitos que se refletem fora do universo virtual. A falta de regulamentação torna a rede um espaço fértil para crimes de ódio, o que teoricamente começaria a ser combatido a partir da aprovação do Marco Civil da Internet. Porém, no caso da violência contra a mulher no mundo virtual a situação tem elementos mais peculiares. (FÓRUM, 2013).

Segundo a autora o número de mulheres que têm suas imagens íntimas divulgadas digitalmente por vingança ou humilhação está crescendo, geralmente causado por ex-parceiros que não aceitam o fim do relacionamento. Esse material rapidamente se espalha online, gerando uma "histeria coletiva", com julgamentos e comentários que intensificam a violência contra as vítimas, afetando tanto suas vidas virtuais quanto cotidianas.

O feminicídio 2.0 seria a forma híbrida que esse crime assumiu com o advento da tecnologia e revitimização da mulher na Sociedade em Rede, tendo em vista a amplificação das informações que transitam no ciberespaço e o impacto que geram fora dele.

> O feminicídio é algo que vai além da misoginia, criando um clima de terror que gera a perseguição e morte das mulheres a partir de agressões físicas e psicológicas dos mais variados tipos, como abuso físico e verbal. Ao adicionarmos o conceito "2.0", podemos sinteticamente nos referir a um estágio específico das mídias digitais, onde a interação e participação ativa é a base estruturante, temos uma forma de agressão e de violência contra as mulheres sem precedentes na história. A rapidez, o impacto e a amplificação de tudo que transita nas mídias digitais está revelando um lado sórdido, ao ser utilizado para expor, humilhar e prejudicar mulheres e adolescentes. (FÓRUM, 2013).

Na Sociedade em Rede não há uma dicotomia entre os acontecimentos que ocorrem dentro e fora das mídias sociais, eles se retroalimentam. Conquanto, se uma mulher sofre a prática de *Porn Revange,* indubitavelmente essa violência será difundida fora das redes sociais e plataformas digitais. A nossa legislação a reconhece como "Vingança Pornô", versado na Lei nº 13.718/2018:

> Art. 218-C. Oferecer, trocar, disponibilizar, transmitir, vender ou expor à venda, distribuir, publicar ou divulgar, por qualquer meio - inclusive por meio de comunicação de massa ou sistema de informática ou telemática -, fotografia, vídeo ou outro registro audiovisual que contenha cena de estupro ou de estupro de vulnerável ou que faça apologia ou induza a sua prática, ou, sem o consentimento da vítima, cena de sexo, nudez ou pornografia.

Contamos outros dispositivos legais relacionados aos crimes digitais, *verbi gratia*, a Lei Carolina Dieckmann (Lei nº 12.737/2012), essa legislação surgiu após a exposição indevida de fotos da atriz Carolina Dieckmann. É que tipificado como crime a invasão de dispositivos eletrônicos para obtenção de dados:

> No Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita.

Por conseguinte, a Lei Rose Leonel (Lei 13.772/2018) em homenagem à mulher que se tornou símbolo do combate à violência e à violência o assédio sexual e a violência de gênero no mundo digital, incluindo *deepFake,* técnica de alterar um vídeo ou foto com de IA. Em sua maioria, utilizado para atingir as mulheres criando conteúdo falso sexual e desnudando-as:

> Art. 216-B . Produzir, fotografar, filmar ou registrar, por qualquer meio, conteúdo com cena de nudez ou ato sexual ou libidinoso de caráter íntimo e privado sem autorização dos participantes: Pena - detenção, de 6 (seis) meses a 1 (um) ano, e multa. Parágrafo único. Na mesma pena incorre quem realiza montagem em fotografia, vídeo, áudio ou qualquer outro registro com o fim de incluir pessoa em cena de nudez ou ato sexual ou libidinoso de caráter íntimo.

A Rose Leonel, jornalista, teve a sua intimidade exposta pelo ex-noivo. Ela teve suas fotos divulgadas em sites brasileiros e internacionais, junto com o telefone dela e do filho

pequeno. Em entrevista à Rádio Senado em 2017, ela descreveu o que aconteceu como "morte civil", pois a exposição resultou em sua exclusão social e marginalização, tornando-a uma persona non grata em sua comunidade e transformando radicalmente sua vida. (BRASIL, 2023).

Outrossim, no ano passado foi criada a Lei nº 14.532/2023, que incluiu na Lei nº 7.716/1989, de crimes resultantes de discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional, a equiparação da injúria racial ao crime de racismo. A nova lei também estabelece punições para discriminação e discursos de ódio na internet, na locução do "art. 20, § 2º: Se qualquer dos crimes previstos neste artigo for cometido por meio de comunicação social, publicação em redes sociais, rede mundial de computadores ou qualquer outra forma de publicação, a pena será de reclusão de dois a cinco anos, além de multa".

Importa destacar e enaltecer, sem reduzir a importância das outras normas, a Lei do Marco Civil da Internet (12.965/2014) que implanta os direitos e deveres no uso da internet, adicionando proteção à privacidade e responsabilização de provedores em casos de conteúdos que transgridam os direitos das mulheres, como o compartilhamento não autorizado de imagens.

Entre de 2019 até 2022, o relatório do Conselho Nacional de Justiça (CNJ) conseguiu apurar que o Brasil registra quatro processos judiciais referentes ao crime divulgação de registros íntimos ou de nudez de terceiros por dia. A Defensora Pública Jeritza Braga, atesta:

> Em grande parte destas situações onde o crime acontece, a maioria das vítimas são as mulheres – apesar de que os homens também podem ser vítimas. Mas, em termos de números, são as mulheres que estão neste maior número justamente pela erotização dos corpos femininos. Em muitos desses casos, a mulher autoriza o conteúdo, a gravação, a foto do seu corpo a um indivíduo, mas ela não autoriza esse compartilhamento. E o crime se configura justamente nesta situação. Quando você, sem autorização, decide compartilhar e divulgar as mensagens, fotos ou vídeos recebidos de modo privado. (DEFENSORIA PÚBLICA DO CEÁRA, 2023).

No caso concreto infracitado, uma mulher teve, sem autorização, suas fotos íntimas divulgadas em um grupo de *WhatsApp* composto apenas por homens. O tribunal reconheceu que tal ato é ilícito, configurando uma violação dos direitos da personalidade da autora, especialmente no que se refere à proteção da sua imagem. A vítima é mãe de uma criança de 9 anos e trabalha na área escolar. Ela informou que os efeitos da conduta do réu foram extremamente lesivos, visto que ele se aproveitou de um momento de fragilidade e de sua confiança para a expor de forma vexatória.

> APELAÇÃO CÍVEL. DIVULGAÇÃO, SEM AUTORIZAÇÃO, EM GRUPO DE WHATSAPP COMPOSTO APENAS DE HOMENS, DE FOTOS ÍNTIMAS. ATO ILÍCITO CONFIGURADO. DEVER DE REPARAÇÃO. QUANTUM INDENIZATÓRIO. SITUAÇÃO ECONÔMICA DO OFENSOR. MINORAÇÃO.

> 1.Os direitos da personalidade qualificam-se por seu caráter personalíssimo e, no que diz respeito à imagem, sua proteção reside em facultar ao indivíduo o direito de refutar sua divulgação, porquanto lhe é exclusiva a faculdade de uso e disposição. 2.Adivulgação, via WhatssApp, de fotografias retratando a intimidade da autora sem que tenha sido dada qualquer autorização, constitui ato ilícito e enseja o dever de indenizar. A conduta é agravada quando as imagens são captadas em momento de fragilidade (sono), eis que demonstra o grau de confiança obtido pelo ofensor antes da prática do ilícito. 3.Dano moral ipso facto, dispensando que a vítima demonstre o abalo sofrido. 4.Afixação do valor do quantum indenizatório pela ofensa moral fica adstrita ao exame das circunstâncias e das consequências do fato, observando-se os critérios da razoabilidade e da proporcionalidade. Recurso conhecido e parcialmente provido. (BRASIL. Tribunal de Justiça do Distrito Federal e Territórios. Acórdão nº 1134314, Relator: Des. Carlos Rodrigues. 6ª Turma Cível. Data de julgamento: 17 out. 2018. Publicado no DJe: 6 nov. 2018.).

Embora haja legislação vigente que busca combater essas discriminações, sua efetividade não tem logrado resultados esperados. Na análise jurisprudencial, observa-se que, mesmo quando são determinadas sentenças de indenização, os valores atribuídos costumam ser minorados, o que reflete na vítima uma sensação de impunidade ou não reparação do dano.

2 O CONTO DA IA

A força motriz da violência online contra a mulher é a cultura do patriarcado, que suprime a existência da mulher como não a vendo como um sujeito de direito na sociedade. O enfoque na concepção de "O Conto da IA" serve como uma crítica às discriminações algorítmicas que afetam a vida das mulheres, revelando um cenário em que as tecnologias que deveriam empoderar se tornam, muitas vezes, instrumentos de opressão e violência. Por meio dessa lente, expõe-se a interseção entre tecnologia, gênero e direitos humanos, evidenciando os desafios que as mulheres enfrentam na era digital.

Em uma passagem do livro de Atwood (2017, p. 11), a personagem Offred, uma aia, profere a frase: “Nós ansiávamos pelo futuro. Como foi que aprendemos aquilo, aquele talento pela insaciabilidade?”. O anseio pelo futuro, embebido de novas tecnologias e praticidades, é algo que nós, na Sociedade em Rede, constantemente buscamos. No entanto, a que preço essa evolução custaria para as mulheres?

A tecnologia gera uma matriz com diversos benefícios e facilidades para a sociedade como um todo, mas também se configura como uma fonte para cometer abusos em face das mulheres, considerando sua etnia, raça, idade, orientação sexual, religião e identidade de gênero. As mulheres são alvos de diversos tipos de discriminação algorítmica (UNRIC, 2023).

Todavia, a que preço essa evolução custaria para as mulheres? A tecnologia gera uma matriz com diversos benefícios e facilidades para a sociedade como um todo, mas também é uma fonte para cometer abusos em face das mulheres, com base na sua etnia, raça, idade, orientação sexual, religião e identidade de gênero. As mulheres são alvos de diversos tipos de discriminação algorítmica. (UNRIC, 2023).

No contexto de “O Conto da IA", o presente trabalho se debruçou sobre a relação entre gênero, inteligência artificial e algoritmos, traçando uma linha temporal com a evolução da condição da mulher como sujeito de direitos e a linha tênue entre o ambiente virtual e o mundo real, rompida com o advento da internet e das novas tecnologias. O fato é que, na República de Gilead, todas as mulheres tiveram seus direitos pulverizados e foram submetidas a condições degradantes após uma nova realidade emergir e mudar as regras do jogo.

É importante consignar que, atualmente, estamos passando por uma transformação social com a interação das redes sociais e das Tecnologias da Informação e Comunicação (TICs), que, neste momento, reproduzem comportamentos injustos direcionados ao gênero feminino.

Em "O Conto da IA", temos, no Brasil, um dos capítulos que narra a história da Deputada Federal Tabata Amaral, que foi vítima de *deepfake* e desinformação. Enquanto se dedicava à sua campanha eleitoral, cuja disputa era para a prefeitura de São Paulo, imagens em poses "sensuais" circularam nas redes sociais. A finalidade das montagens era manchar sua imagem perante o eleitorado, o que é irrefutável. O G1 (2024) trouxe em reportagem que uma perícia foi realizada, também com o uso de inteligência artificial, para detectar se a imagem era falsa ou não.

Noutro, celebridades como a atriz Scarlett Johansson e a cantora Taylor Swift também são vítimas de *deepfakes* que são compartilhadas em redes sociais e rapidamente disseminadas, assim como mulheres anônimas. O crime virtual atinge majoritariamente as mulheres, independentemente da classe social, raça ou cor; no entanto, esses fatores podem intensificar a violência online. A vulnerabilidade social da mulher, por conta de seu gênero, é explorada e massificada nas mídias sociais.

Ainda não temos um desfecho para esse conto. O que se sabe é que mulheres têm seus direitos humanos violados por meio da IA e algoritmos nas plataformas digitais. Esse comportamento é um sintoma das chagas que o patriarcado criou em nossa sociedade e incide

sobre todas as mulheres, estas que por sua vez anseiam por um futuro melhor, assim como a personagem Offred, em que a tecnologia não reforce mais preconceitos e discriminações, mas os anule, permitindo que seus direitos humanos sejam respeitados independente do gênero.

CONCLUSÃO

Pode-se concluir que a analogia entre "Conto da Aia" e o " Conto da IA", evidencia-se a persistente luta das mulheres contra a opressão e a instrumentalização dos seus corpos. Enquanto a obra de Margaret Atwood retrata um futuro distópico em que as mulheres são reduzidas a meros instrumentos de reprodução em uma sociedade totalitária, o "Conto da IA", expressão criada para gerar uma reflexão sobre a discriminação algorítmica enfrentada pelas mulheres na era da inteligência artificial e o alerta para os perigos da tecnologia que pode reforçar estereótipos de gênero e perpetuar a violação de seus direitos humanos.

Os algoritmos, muitas vezes, refletem preconceitos existentes na sociedade e, quando aplicados em plataformas digitais, podem resultar em discriminação algorítmica, perpetuando estereótipos de gênero e marginalizando as “vozes” femininas. Isso ressalta a necessidade de uma abordagem crítica em relação à programação e à implementação desses algoritmos, a fim de promover um ambiente online seguro para todas as mulheres.

A mobilização social torna-se imprescindível para enfrentar os preconceitos enraizados que enviesam as estruturas algorítmicas, moldando nossas interações e decisões. A criação de leis como a Rose Leonel e o fortalecimento de normas voltadas à proteção das mulheres no ambiente digital representam avanços cruciais, mas ainda há uma baixa efetividade na aplicação dessas medidas, especialmente no que diz respeito à violência digital. O que pode ser chamado de Feminicídio 2.0, termo cunhado por Brunna Rosa, para traduzir a violência de gênero amplificada por tecnologias e plataformas digitais. Nesse sentido, é vital articular esses desafios à luta por direitos humanos, ampliando a compreensão das violências sofridas pelas mulheres, inclusive no ambiente virtual.

REFERÊNCIAS

ALMEIDA, Caroline de Oliveira. **Posicionamentos doutrinários quanto à natureza da qualificadora do feminicídio**. Jus.com.br, 2019. Disponível em: https://jus.com.br/artigos/64615/posicionamentos-doutrinarios-quanto-a-natureza-da-qualificadora-do-feminicidio. Acesso em: 27 out. 2024.

ARBEX, Daniela. **Holocausto Brasileiro**. 1. ed. São Paulo: Geração Editorial, 2013.

ATWOOD, Margaret. **O conto da AIA**. 1. ed. Rio de Janeiro: Rocco, 2017.

BEAUVOIR, Simone de. **O segundo sexo.** 5. ed. Rio de Janeiro: Nova Fronteira, 2019.

BRASIL. **Código Penal. Lei nº 2.848**, **de 7 de dezembro de 1940.** Atualizado pela Lei nº 13.718, de 24 de setembro de 2018**.** Diário Oficial da União: Brasília, 25 set. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/1940/L2848.htm. Acesso em: 27 out. 2024.

BRASIL. **Constituição da República Federativa do Brasil.** Brasília, 5 out. 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 27 out. 2024.

BRASIL. **Lei nº 11.340, de 7 de agosto de 2006. Cria mecanismos para coibir a violência doméstica e familiar contra a mulher.** Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11340.htm. Acesso em: 24 out. 2024.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos.** Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 21 out. 2024.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.** Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 20 out. 2024.

BRASIL. **Lei nº 13.104, de 9 de março de 2015. Altera o art. 121 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, para prever o feminicídio como circunstância qualificadora do homicídio, e o art. 1º da Lei nº 8.072, de 25 de julho de 1990, para incluir o feminicídio no rol dos crimes hediondos.** Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13104.htm.

BRASIL. **Lei nº 13.718, de 24 de setembro de 2018. Altera o Código Penal para tipificar os crimes de importunação sexual e divulgação de cena de estupro.** Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13718.htm. Acesso em: 22 out. 2024.

BRASIL **Lei nº 13.718, de 24 de setembro de 2018. Altera o Código Penal para tipificar a divulgação de imagens ou vídeos que contenham cenas de sexo ou nudez sem autorização da pessoa retratada.** Diário Oficial da União: Brasília, 25 set. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2018/L13718.htm. Acesso em: 27 out. 2024.

BRASIL. **Lei nº 13.772, de 27 de dezembro de 2018. Altera o Código Penal para tipificar o crime de assédio sexual em ambientes virtuais.** Diário Oficial da União: seção 1, Brasília, DF, 28 dez. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2018/L13772.htm. Acesso em: 27 out. 2024.

BRASIL**. Lei nº 7.716, de 5 de janeiro de 1989. Define crimes resultantes de preconceito de raça ou de cor.** Diário Oficial da União: seção 1, Brasília, DF, 6 jan. 1989. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l7716.htm. Acesso em: 27 out. 2024.

BRASIL. **Lei nº 7.716, de 5 de janeiro de 1989. Define os crimes resultantes de preconceito de raça ou de cor.** Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l7716.htm. Acesso em: 27 out. 2024.

BRASIL. **Senado pode aumentar pena para registro não autorizado de intimidade sexual.** Disponível em: https://www12.senado.leg.br/radio/1/noticia/2023/12/12/senado-pode-aumentar-pena-para-registro-nao-autorizado-de-intimidade-sexual#:~:text=O%20crime%20foi%20tipificado%20em,intimidade%20exposta%20pelo%20ex%2Dnoivo. Acesso em: 27 out. 2024.

BRASIL. Supremo Tribunal Federal. **Constituição de 1988 ampliou espaço das mulheres e garantiu direitos fundamentais.** Portal STF, 2023. Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=495430&ori=1. Acesso em: 27 out. 2024.

BRASIL. Tribunal de Justiça do Distrito Federal e Territórios. **Acórdão nº 1134314, Relator: Des. Carlos Rodrigues. 6ª Turma Cível. Data de julgamento: 17 out. 2018.** Publicado no DJe: 6 nov. 2018. Disponível em: https://pesquisajuris.tjdft.jus.br/IndexadorAcordaos-web/sistj. Acesso em: 20 out. 2024.

BUTLER, Judith. **Problemas de gênero: Feminismo e subversão da identidade.** 20. ed. Rio de Janeiro: Civilização Brasileira, 2020.

CASTELLS, Manuel. **A sociedade em rede.** 2. ed. São Paulo: Paz e Terra, 1999. (Volume 1, A era da informação: economia, sociedade e cultura).

DEFENSORIA PÚBLICA DO CEARÁ. **Exposição de fotos íntimas na internet é crime e gera dores reais às vítimas.** Defensoria CE, 27 out. 2023. Disponível em: https://www.defensoria.ce.def.br/noticia/exposicao-de-fotos-intimas-na-internet-e-crime-e-gera-dores-reais-as-vitimas/. Acesso em: 28 out. 2024.

DHnet – Rede de Direitos Humanos e Cultura. **Código de Manu**. Disponível em: https://www.dhnet.org.br/direitos/anthist/manusrti3.htm#:~:text=420%C2%BA%20Uma%20mulher%20est%C3%A1%20sob,se%20conduzir%20%C3%A0%20sua%20vontade. Acesso em: 20 out. 2024.

DOSTOIÉVSKI, Fiódor. **Crime e Castigo**. São Paulo: Editora 34, 2006.

FIORILLO, C. A. P.; FULLER, G. P.; LIMA, M. A. Aspectos Atuais e Problemáticos no Âmbito da Responsabilidade do Provedor de Serviços em Face do Meio Ambiente Digital no Direito Ambiental Brasileiro e Espanhol. **Revista Internacional Consinter de Direito**, Paraná, Brasil, v. 1, n. 1, p. 65–86, 2015. DOI: 10.19135/revista.consinter.00001.04. Disponível em: https://revistaconsinter.com/index.php/ojs/article/view/377. Acesso em: 27 out. 2024.

FLORESTA, Nísia. **Direitos das mulheres e injustiça dos homens.** São Paulo: Editora Cortez, 1989.

FORBES. **Scarlett Johansson, Taylor Swift e Michael Schumacher: celebridades são principais vítimas da IA.** 2024. Disponível em: https://forbes.com.br/forbes-tech/2024/05/scarlett-johansson-taylor-swift-e-michael-schumacher-celebridades-sao-principais-vitimas-da-ia/. Acesso em: 27 out. 2024.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. **Anuário Brasileiro de Segurança Pública 2023**. Disponível em: https://forumseguranca.org.br/wp-content/uploads/2023/08/anuario-2023-texto-07-o-crescimento-de-todas-as-formas-de-violencia-contra-a-mulher-em-2022.pdf. Acesso em: Acesso em: 27 out. 2024.

G1**. Após fotos íntimas pararem na web, mulher diz sofrer preconceito diário.** Disponível em: https://g1.globo.com/pr/norte-noroeste/noticia/2013/08/apos-fotos-intimas-pararem-na-web-mulher-diz-sofrer-preconceito-diario.html. Acesso em: 27 out. 2024.

G1. **É fake? Foto de Tabata Amaral em pose sensual trata-se de deepfake.** São Paulo, 15 set. 2024. Disponível em: https://g1.globo.com/fato-ou-fake/sao-paulo/noticia/2024/09/15/e-fake-foto-de-tabata-amaral-em-pose-sensual-trata-se-de-deepfake.ghtml. Acesso em: 27 out. 2024.

GONZAGA, Christiano. **Manual de Criminologia.** 2. ed. São Paulo: Saraiva Jur, 2020.
KHOO, Cynthia. **Deplatforming Misogyny: A report on the impact of misogyny in online spaces**. Leaf, Faej, 2021. Disponível em: https://www.leaf.ca/wp-content/uploads/2021/04/Full-Report-Deplatforming-Misogyny.pdf. Acesso em: 27 out. 2024.

MIGALHAS. **Veja principais alterações da lei que aumenta pena para feminicídio**. Migalhas, 24 out. 2023. Disponível em: https://www.migalhas.com.br/quentes/417174/veja-principais-alteracoes-da-lei-que-aumenta-pena-para-feminicidio. Acesso em: 27 out. 2024.
NAÇÕES UNIDAS. **A ONU pede que os Estados adotem legislação para proteger as mulheres contra a violência cibernética**. United Nations News, 19 jul. 2023. Disponível em: https://news.un.org/pt/story/2023/07/1817092. Acesso em: 27 out. 2024.

NUCCI, Guilherme de S. **Curso de Direito Penal: Parte Especial: Arts. 121 a 212 do Código Penal. v.2**. 7th ed. Rio de Janeiro: Forense, 2023. E-book. ISBN 9786559647217. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9786559647217/. Acesso em: 28 out. 2024.

PIOVESAN, Flávia. **Direitos Humanos e o Direitos Constitucional Internacional.** 12. ed. São Paulo: Saraiva, 2011.

PIOVESAN, Flávia. **Temas de direitos humanos**. 12th ed. Rio de Janeiro: Saraiva Jur, 2023. E-book. p.428. ISBN 9786555599619. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9786555599619/. Acesso em: 27 out. 2024.

SILVA, Ellen Maria Rocha da. **O impacto da pandemia no enfrentamento da violência doméstica contra a mulher no Brasil.** Revista Jurídica OAB Tatuapé, v. 2, n. 2, 2023. Disponível em: https://revista.oabtatuape.org.br/index.php/revista/article/view/63/39. Acesso em: 27 out. 2024.

TASO, Fernanda Tiemi de S.; REIS, Valéria Q.; MARTINEZ, Fábio Viduani. Discriminação Algorítmica de Gênero: Estudo de Caso e Análise no Contexto Brasileiro. In: **IV Workshop sobre as Implicações da Computação na Sociedade (WICS)**, João Pessoa, PB, 2023. Anais... Sociedade Brasileira de Computação, 2023. DOI: 10.5753/wics.2023.229980. Disponível em: https://www.researchgate.net/publication/373139729_Discriminacao_Algoritmica_de_Genero_Estudo_de_Caso_e_Analise_no_Contexto_Brasileiro. Acesso em: 28 out. 2024.

UNITED NATIONS REGIONAL INFORMATION CENTRE FOR WESTERN EUROPE (UNRIC). **Como a violência de gênero facilitada pela tecnologia afeta as mulheres**. Disponível em: https://unric.org/pt/como-a-violencia-de-genero-facilitada-pela-tecnologia-afeta-as-mulheres/. Acesso em: 28 out. 2024.

UNIVERSITY OF MELBOURNE; UNITED NATIONS POPULATION FUND. **Measuring technology-facilitated gender-based violence: a discussion paper**. 2023. Disponível em: https://www.coe.int/documents/75383286/207520194/UNFPA_Measuring+TF+GBV_+A+Discussion+Paper_FINAL.pdf/23807c3c-094f-0860-baaa-a0f6133bb10b?t=1681812227233. Acesso em: 27 out. 2024.

VICENTE, Gil. **A farsa de Inês Pereira**. São Paulo: Editora 34, 2005. (Coleção Teatro de Gil Vicente).

WOLF, Naomi. **O mito da beleza**: como as imagens de beleza são usadas contra as mulheres. 14. ed. Rio de Janeiro: Rosa dos Tempos, 2020.

7 Information Society and Law
FMU CENTRO UNIVERSITÁRIO

FAKE NEWS E SOCIEDADE DA INFORMAÇÃO: AS CONDUTAS DO CANDIDATO A PREFEITURA DE SÃO PAULO PABLO HENRIQUE MARÇAL NA ELEIÇÃO MUNICIPAL DE SÃO PAULO DE 2024

FAKE NEWS AND INFORMATION SOCIETY: THE CONDUCT OF THE CANDIDATE FOR MAYOR OF SÃO PAULO PABLO HENRIQUE MARÇAL IN THE 2024 MUNICIPAL ELECTION OF SÃO PAULO

Ronny Max Machado[1]; João Francisco Mantovanelli[2]

Resumo: O presente resumo expandido, por meio da metodologia da revisão bibliográfica e análise de notícias, tem por objetivo apresentar as condutas desinformadoras do candidato Prefeitura da Cidade de São Paulo Pablo Henrique Marçal no ano de 2024 e suas implicações jurídicas.
Palavras-chave: Sociedade da Informação; Eleições; Prefeitura.

Abstract: This expanded summary, using the methodology of bibliographic review and news analysis, aims to present the misleading conduct of the candidate for Mayor of the City of São Paulo Pablo Henrique Marçal in 2024 and its legal implications.
Keywords: Information Society; Elections; City Hall.

INTRODUÇÃO

De acordo com a Lei 13.488/2017, em seu artigo 57 alínea C de forma taxativa e exegética aduz: "É vedada a veiculação de qualquer tipo de propaganda eleitoral paga na internet, excetuado o impulsionamento de conteúdos, desde que identificado de forma inequívoca como tal e contratado exclusivamente por partidos, coligações e candidatos e seus representantes". O presente resumo expandido, através da metodologia da revisão bibliográfica e análise de notícias, tem por finalidade apresentar as condutas desinformadoras do candidato

[1] Mestre em Direito da Sociedade da Informação pelo Centro Universitário das Faculdades Metropolitanas Unidas. São Paulo. Estado de São Paulo. Brasil. Pesquisador junto ao Programa de Mestrado em Direito da Sociedade da Informação pelo Centro Universitário das Faculdades Metropolitanas Unidas. São Paulo. Estado de São Paulo. Brasil

[2] Graduado em Direito pela Faculdade de Americana -FAM (2009-2013). Pós-graduado em Direito Urbanístico e Meio Ambiente pela Damásio Educacional (2021-2022). Pesquisador junto ao Programa de Mestrado em Direito da Sociedade da Informação pelo Centro Universitário das Faculdades Metropolitanas Unidas. São Paulo. Estado de São Paulo. Brasil.

Prefeitura da Cidade de São Paulo Pablo Henrique Marçal no ano de 2024 e suas implicações jurídicas.

DISCUSSÕES E RESULTADOS

Na matéria jornalística publicada pelo site de notícias Hora do Povo, no dia 11 de setembro de 2024 revela: Cai outra farsa de Marçal: nenhum indício de que sofreu atentado, informa Secretaria:

> Não há nenhum indício de que Marçal tenha sido alvo de ataques em comício", afirmou a Secretaria de Segurança Pública de São Paulo. A encenação se deu quando uma candidata a vereadora do Psol, que estava em campanha no mesmo local do comício, tentou entregar ao candidato, um boneco do pinóquio, caracterizando as mentiras ditas por ele durante a campanha. Entre elas a ocultação de sua condenação e prisão por participar de uma quadrilha de roubos a bancos. No Instagram, no mesmo dia do episódio, a candidata do Psol, Carol Iara, publicou vídeo e nota em que aparece sendo "perseguida por um segurança de Pablo Marçal". Iara informou que passou o dia em campanha na Zona Leste e conta que Marçal apareceu e ela tentou entregar a ele um boneco de Pinóquio (feito de isopor). Ela comentou também que foi perseguida e que saiu rapidamente do local, "porque a extrema direita é bastante truculenta, e bastante mentirosa". Na montagem da farsa, Marçal produziu e disseminou um áudio que teria sido vazado da Polícia Militar de São Paulo (PMSP). No áudio falso, dois homens discutem e caracterizam uma ocorrência como "tentativa de homicídio". A polícia desmentiu o áudio. (Hora do Povo,2024).

No fatídico debate eleitoral promovido pela Tv. Cultura, no dia 15 de setembro de 2024, Pablo Marçal acusou sem prova ilibada e sem condenação cível e/ou criminal e sem uma transitada e julgada ou em andamento de estupro cometido pelo jornalista José Luiz Datena contra uma repórter, que ao ser chamado de estuprador e na gíria marginal de *Jack*, o revidou com uma cadeirada repelindo com injusta provocação que atingiu sua honra subjetiva. Em seu legítimo poder de retorsão. Como relata a reportagem pelo site Brasil de Fato, publicada no dia 16/09/2024: "Acúmulo de desaforos': cadeirada de Datena foi resposta ao rebaixamento da política por Marçal (Hora do Povo,2024):

> A cadeirada de Datena em Marçal veio após o coach relembrar um caso, já encerrado na Justiça, em que o tucano foi acusado de assédio sexual. Rudá Ricci, cientista político, lamentou o episódio, mas disse que o candidato do PRTB está conectado com o que o eleitorado tem esperado da eleição. "É uma minoria dos brasileiros que quer ver propostas, porque a maioria acha que os políticos são safados, então eles querem ver circo. Além disso, a juventude quer esse espírito provocativo e o campo progressista não está preparado para isso", argumenta Ricci. Para o especialista, a tática do coach é uma novidade que deverá ser permanente na política e não pode ser interrompida. (Carvalho,2024).

E às injustas acusações teve como vítima um outro candidato, Guilherme Boulos sobre a utilização de uma outra pessoa com nome homônimo ao de Boulos, como evoca a matéria do

site jornalístico Metrópoles: “Marçal usa processo de homônimo de Boulos para embasar ataque a rival”. Se não bastasse esta imputação de crime de posse de droga ilícita como a cocaína, Pablo Marçal mediante um laudo psiquiátrico falso para envolver uma suposta ligação de Boulos sendo usuário de drogas na véspera de eleição municipal como desvendado ao site G1 de notícias: “Perícia da PF conclui que assinatura de médico em laudo publicado por Marçal contra Boulos é falsa (Metrópoles,2024)”:

> Os peritos da PF investigaram e compararam várias assinaturas ao longo de vários anos do médico José Roberto de Souza, CRM 17064-SP, que aparece como o responsável pelo suposto documento. O médico morreu em 2022 e, segundo a filha, a oftalmologista Aline Garcia Souza, o pai nunca trabalhou na clínica Mais Consulta, na cidade de São Paulo, e jamais fez esse tipo de atendimento clínico de pessoas com dependência química. Na conclusão grafotécnica, os peritos científicos da PF afirmaram que as duas assinaturas não foram produzidas pela mesma pessoa. “Verificou-se a prevalência das dissimilaridades entre a assinatura questionada e os padrões apresentados, tanto nas formas gráficas, quanto em suas gêneses, não havendo evidências de que tais grafismos tenham sido escritos por uma mesma pessoa. As evidências suportam fortemente a hipótese de que os manuscritos questionados não foram produzidos pela mesma pessoa que forneceu os padrões”, disseram os peritos (Tavares,2024).

Pablo Marçal também veiculou crime contra o atual prefeito da cidade de São Paulo e candidato à reeleição Ricardo Nunes sobre alguns funcionários públicos do município paulistano de terem ido no dia 07 de setembro de 2024 à avenida Paulista e levaram uma bandeira contendo a seguinte frase: “Pablo Marçal presidente do Brasil”. Como fora demonstrado pelo site Agenda do Poder, publicado no dia 09 de setembro de 2024: “Bandeira do Brasil na Av. Paulista escrita com ‘Pablo Marçal presidente do Brasil’ gera nova disputa entre ex-coach e Nunes”:

> Durante o ato do último dia 7 de setembro na Avenida Paulista, uma bandeira com a frase “Bolsonaro parou. Marçal começou. Pablo Marçal presidente do Brasil” gerou uma disputa entre os candidatos Pablo Marçal (PRTB) e Ricardo Nunes (MDB). Marçal alega que funcionários da Prefeitura de São Paulo foram responsáveis por estender a bandeira, enquanto Nunes negou a acusação, chamando Marçal de “mentiroso” e afirmando que levará o caso à polícia. Em vídeo publicado no Instagram, Marçal acusou a prefeitura de estar envolvida no ato, sugerindo que a bandeira foi colocada para gerar atrito entre ele e Jair Bolsonaro. Nunes, por sua vez, rebateu, afirmando que Marçal “não respeita Bolsonaro” e que as imagens usadas pelo adversário foram distorcidas. Segundo Nunes, os funcionários públicos estavam, na verdade, retirando a bandeira no fim da manifestação para realizar a limpeza da avenida. Em nota, a campanha de Nunes declarou que ele pedirá a abertura de um inquérito policial e direito de resposta à Justiça Eleitoral. (Fernandes, 2024).

E divulgou também Fake News contra a candidata Tábata Amaral ao alegar nas redes sociais e em alguns debates televisivos sobre o suicídio do pai de Tábata que ela era a responsável pela morte, porque ela abandonara o Brasil na mesma época em que seu pai

cometera o suicídio. Como consta estas informações veiculadas ao site de notícias online Metrópoles do dia 09/09/2024: “Tabata rebate ataque de Marçal sobre seu pai: “É nojento, perverso”:

> Em entrevista para um podcast da revista Isto É, Marçal afirmou que o pai da deputada morreu porque ela o abandonou no Brasil para viajar aos Estados Unidos. “Se a pessoa foi estudar em Harvard, às mil maravilhas, enquanto eu estava aqui trabalhando pra pagar [a faculdade]; eu passei por mais problemas que ela. (…) Eu também tive um pai que foi alcoólatra, mas a família ajudou e ele deixou o alcoolismo. O pai dela, ela foi para Harvard, ele acabou morrendo. Igual imagino que ela pode fazer com o povo de São Paulo”, alegou. Tabata afirmou no vídeo que “essa baixaria do Pablo Marçal sequer faz sentido”, porque ela estava no Brasil quando o próprio pai morreu. “Na mesma semana que eu fui aceita em Harvard, ele cometeu suicídio”, contou a deputada. “Eu era muito nova, sofri muito e cheguei a desistir de ir pros Estados Unidos. Eu fui. Mas nunca deixei de cuidar da minha família. (Sales,2024).

CONCLUSÃO

Sob a ótica conclusiva, tem-se como principal característica das Fake News é a geração e propagação de informações, advindas de qualquer lugar do mundo, em tempo quase que real e de forma inédita na história da tecnologia (Barreto Junior,2020. p. 100-127.)

Essas Fake News praticadas por Pablo Henrique Marçal fomentam a cultura de ódio contra candidatos que concorrem ao cargo de prefeito e que atente ao Estado Democrático de Direito ao disseminar de forma consistente com o grande número de envios de conteúdos falsos contra os seus adversários políticos infringindo ao artigo 359, alínea O do Código Penal brasileiro, in verbis: “Promover ou financiar, pessoalmente ou por interposta pessoa, mediante uso de expediente não fornecido diretamente pelo provedor de aplicação de mensagem privada, campanha ou iniciativa para disseminar fatos inverídicos, e que sejam capazes de comprometer a higidez do processo eleitoral. Nos estudos de Rogério Sanches Cunha (2024, p. 1336-1337) reforça:

> A promoção ou o financiamento de campanha ou iniciativa para disseminar fatos mentirosos potencialmente danosos a qualquer destas fases pode caracterizar o crime. Alertarmos que o crime contra a honra cometido no contexto da comunicação enganosa em massa ficará absorvido. É o dolo na vontade consciente uma das ações nucleares. Considerando que o tipo penal contém a expressão “para disseminar fatos que *sabe* inverídicos”, o agente que promove ou financia a disseminação deve ter a certeza da inverdade. (Cunha, 2024, p. 1336-1337).

Segundo, Khalil Coltro, Barreto e Machado(2024) “o direito à liberdade expressão e manifestação são de natureza fundamental para o exercício da democracia” contudo, as condutas utilizadas para ferir a honra-moral dos candidatos políticos não condizem por liberdade de expressão e de livre opinião uma vez que venha a agredir a personalidade e a

dignidade nos direitos de imagem, material, moral e familiar, além de incitar a cultura de intolerância e de ódio, incide estas condutas maléficas em crimes contra a honra porque engloba a injúria, calúnia e a difamação.

REFERÊNCIAS

BARRETO JUNIOR, Irineu Francisco. Fake News e Discurso do Ódio: estratégia de guerra permanente em grupos de WhatsAppIn: RAIS, Diogo (coord.). **FAKE NEWS: a conexão entre desinformação e o Direito**.2. ed. São Paulo: Thomson Reuters Brasil, 2020

BRASIL. Lei nº 13.488, de 6 de outubro de 2017. **Altera as Leis n º 9.504, de 30 de setembro de 1997 (Lei das Eleições), 9.096, de 19 de setembro de 1995, e 4.737, de 15 de julho de 1965 (Código Eleitoral), e revoga dispositivos da Lei nº 13.165, de 29 de setembro de 2015 (Minirreforma Eleitoral de 2015), com o fim de promover reforma no ordenamento político-eleitoral.** Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2017/Lei/L13488.htm Acesso em:13/10/2024

BRASIL. Decreto-Lei n. 2.848, de 7 de Dezembro de 1940.**Código Penal.** Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm Acesso em: 13/10/2024

CARVALHO, Igor. Acúmulo de desaforos': cadeirada de Datena foi resposta ao rebaixamento da política por Marçal. **Brasil de Fato.** 16 de Setembro de 2024 às 16:20. Disponível em: https://www.brasildefato.com.br/2024/09/16/acumulo-de-desaforos-cadeirada-de-datena-foi-resposta-ao-rebaixamento-da-politica-por-marcal Acesso no dia 11/10/2024 às 20:39.

CUNHA, Rogério Sanches. **Manual de direito penal**: Parte especial. 17 ed. São Paulo: Juspdvim, 2024.

FERNANDES, César. Bandeira do Brasil na Av. Paulista escrita com ‘Pablo Marçal presidente do Brasil’ gera nova disputa entre ex-coach e Nunes. **Agenda do Poder.** Domingo, 13 de Outubro de 2024.Disponível em: https://agendadopoder.com.br/bandeira-do-brasil-na-av-paulista-escrita-com-pablo-marcal-presidente-do-brasil-gera-nova-disputa-entre-marcal-e-nunes/ Acesso dia 11/10/2024 às 20:24

HORA DO POVO. Cai outra farsa de Marçal: nenhum indício de que sofreu atentado, informa Secretaria. **Hora do Povo.** Publicado em 11 de setembro de 2024. Disponível em: https://horadopovo.com.br/cai-outra-farsa-de-marcal-nenhum-indicio-de-que-sofreu-atentado-informa-secretaria/ Acesso dia 11/10/2024 às 20:24

MACHADO, Ronny Max; BARRETO, Osmar Fernando Gonçalves; COLTRO, Rafael Khalil. DIREITOS HUMANOS FUNDAMENTAIS, POPULISMO E DEMOCRACIA NO BRASIL: UMA ANÁLISE CRÍTICA. **Revista Jurídica OAB Tatuapé**, v. 3, n. 2, 2024.

METRÓPOLES. Marçal usa processo de homônimo de Boulos para embasar ataque a rival. **Metrópoles.** 28/08/2024 15:52, atualizado 28/08/2024 21:16. Disponível em: https://www.metropoles.com/sao-paulo/marcal-usa-processo-de-homonimo-de-boulos-para-embasar-ataque-a-rival Acesso dia 11/10/2024 às 20:24

SALES, Bruna. Tabata rebate ataque de Marçal sobre seu pai: "É nojento, perverso" **Metrópoles.** 05/07/2024 11:52, atualizado 09/09/2024 23:48. Disponível em: https://www.metropoles.com/sao-paulo/tabata-rebate-ataque-marcal-sobre-pai Acesso dia 11/10/2024 às 20:24

TAVARES, Bruno. Perícia da PF conclui que assinatura de médico em laudo publicado por Marçal contra Boulos é falsa. **G1.** 07/10/2024 16h22 Atualizado há 5 dias. Disponível em: https://g1.globo.com/sp/sao-paulo/eleicoes/2024/noticia/2024/10/07/pericia-da-pf-conclui-que-assinatura-de-medico-em-laudo-publicado-por-marcal-contra-boulos-e-falsa.ghtml Acesso dia 11/10/2024.

7 Information Society and Law
FMU CENTRO UNIVERSITÁRIO

DISCRIMINAÇÃO E VIOLAÇÕES DE DIREITOS HUMANOS PELO ALGORITMO NOS ESTADOS UNIDOS

ALGORITHMIC DISCRIMINATION AND HUMAN RIGHTS VIOLATIONS IN THE UNITED STATES

Bruna Matos de Souza[1]; Claudio Luiz de Carvalho[2]

Resumo: Este estudo examina a discriminação algorítmica e suas implicações para os direitos humanos nos Estados Unidos, com base em análise qualitativa de casos judiciais, relatórios de organizações civis e literatura especializada. A pesquisa destaca três áreas críticas: o uso do algoritmo COMPAS no sistema judicial criminal, tecnologias de reconhecimento facial e algoritmos de crédito. O caso Loomis v. Wisconsin evidenciou o viés racial do COMPAS, atribuindo pontuações de risco mais elevadas a réus negros, mesmo em condições semelhantes às de réus brancos, o que gerou debates sobre transparência e devido processo. No campo do reconhecimento facial, casos como o de Robert Williams demonstram maior probabilidade de erro na identificação de pessoas negras, levando a detenções injustas e discussões sobre a constitucionalidade do uso policial dessa tecnologia. Quanto aos algoritmos de crédito, denúncias contra empresas como Apple e Amazon revelam discriminação indireta de gênero e raça, reforçando desigualdades estruturais. Apesar da existência de leis como a Equal Credit Opportunity Act e a Lei dos Direitos Civis de 1964, a opacidade algorítmica dificulta a responsabilização e o combate à discriminação. Conclui-se que a ausência de regulamentação federal abrangente e mecanismos efetivos de auditoria e transparência perpetua práticas discriminatórias. Recomenda-se a adoção de políticas públicas e diretrizes éticas robustas para garantir a igualdade, a dignidade e a não discriminação, alinhando o uso de tecnologias de inteligência artificial aos princípios constitucionais e aos tratados internacionais de direitos humanos.
Palavras-chave: Discriminação algorítmica; Direitos Humanos; Inteligência Artificial; Justiça Social; Estados Unidos

Abstract: This study examines algorithmic discrimination and its implications for human rights in the United States, based on a qualitative analysis of court cases, civil society reports, and specialized literature. The research highlights three critical areas: the use of the COMPAS algorithm in the criminal justice system, facial recognition technologies, and credit scoring algorithms. The Loomis v. Wisconsin case revealed the racial bias of COMPAS, which assigned higher risk scores to Black defendants even under conditions similar to those of White defendants, sparking debates on transparency and due process. In facial recognition, cases such as Robert Williams' wrongful arrest demonstrate a higher likelihood of misidentifying Black

[1] Mestranda em Direito pelo Centro Universitário das Faculdades Metropolitanas Unidas – FMU/SP. Especialista em Conflitos Internacionais e Globalização, pela UNIFESP. Lattes: http://lattes.cnpq.br/9407280259256928
[2] Mestre em Economia Aplicada pela Universidade Federal de Juiz de Fora, mestrando em Direito pelo Centro Universitário das Faculdades Metropolitanas Unidas – FMU/SP. Especialista em Gestão Tributária pela ESALQ – USP. Lattes: http://lattes.cnpq.br/7723775631450090.

individuals, prompting discussions on the constitutionality of police use of such technology. Regarding credit algorithms, complaints against companies such as Apple and Amazon reveal indirect gender and racial discrimination, reinforcing structural inequalities. Although laws such as the Equal Credit Opportunity Act and the 1964 Civil Rights Act exist, algorithmic opacity hinders accountability and the fight against discrimination. The study concludes that the absence of comprehensive federal regulation and effective mechanisms for auditing and transparency perpetuates discriminatory practices. It recommends the adoption of robust public policies and ethical guidelines to ensure equality, dignity, and non-discrimination, aligning the use of artificial intelligence technologies with constitutional principles and international human rights treaties.
Keywords: Algorithmic discrimination; Human Rights; Artificial Intelligence; Social Justice; United States

INTRODUÇÃO

A utilização de algoritmos tem se tornado uma prática comum em setores variados, desde a administração pública até serviços financeiros e de saúde. Contudo, a crescente dependência de sistemas automatizados e de inteligência artificial (IA) trouxe à tona um problema crítico: a discriminação algorítmica, que pode resultar em violações de direitos humanos. Em casos recentes, verificou-se que algoritmos utilizados por instituições governamentais e empresas privadas nos Estados Unidos violaram direitos fundamentais, refletindo preconceitos raciais, sociais e econômicos que amplificam desigualdades. Este estudo analisa casos específicos processados judicialmente nos EUA, expondo as principais falhas desses algoritmos e o tratamento jurídico dado a essas violações.

Os algoritmos são frequentemente retratados como instrumentos de eficiência e neutralidade. No entanto, é inegável que, ao serem programados, refletem vieses dos dados utilizados e dos desenvolvedores. Essa falta de neutralidade coloca em risco direitos fundamentais e impacta desproporcionalmente minorias raciais e sociais. O problema central deste estudo reside em como tais vieses se traduzem em decisões discriminatórias e em violações de direitos humanos, como o direito à igualdade e à dignidade. Este trabalho visa entender em que medida esses vieses são identificados e penalizados pelo sistema judicial estadunidense e examinar os limites das abordagens regulatórias e judiciais ao fenômeno da discriminação algorítmica.

Assim, para investigar os impactos discriminatórios dos algoritmos, adotou-se uma abordagem qualitativa, baseada em análise de documentos e revisões bibliográficas de casos notórios nos Estados Unidos. São analisados processos judiciais e relatórios de organizações de

direitos civis, buscando compreender como as cortes americanas interpretam as infrações de direitos humanos no contexto algorítmico. Complementarmente, explora-se a literatura especializada para delimitar as diretrizes éticas e legais aplicadas.

O uso de algoritmos para tomada de decisões impacta uma ampla gama de direitos humanos, incluindo o direito à privacidade, à igualdade e à não discriminação. Segundo a Declaração Universal dos Direitos Humanos, todas as pessoas têm direito a uma proteção igual perante a lei, sem discriminação. A Convenção Internacional sobre a Eliminação de Todas as Formas de Discriminação Racial, da ONU, enfatiza que qualquer ação que afete desigualmente as pessoas com base em raça ou etnia constitui discriminação. Todavia, no contexto dos EUA, os direitos civis e a proteção contra discriminação encontram respaldo na legislação doméstica, como a Lei dos Direitos Civis de 1964 e a Lei de Igualdade de Crédito, que visa combater a discriminação em contextos de crédito.

CASOS DE DISCRIMINAÇÃO ALGORÍTMICA NOS EUA

1. COMPAS e o Sistema Judicial Criminal

Em um caso amplamente discutido, o algoritmo COMPAS (Correctional Offender Management Profiling for Alternative Sanctions) foi utilizado para avaliar a reincidência de criminosos. Desenvolvido pela empresa Northpointe, o COMPAS foi adotado por tribunais estaduais e federais para auxiliar nas decisões de sentenças e na concessão de liberdade condicional. Contudo, estudos mostraram que o COMPAS exibia um viés racial significativo. Pesquisas indicaram que o sistema atribuía pontuações de risco mais altas a réus negros em comparação aos réus brancos, mesmo em condições semelhantes, configurando uma discriminação racial. O caso Loomis v. Wisconsin, analisado pela Suprema Corte de Wisconsin, questionou a imparcialidade do algoritmo, mas a corte concluiu que o COMPAS era apenas um dos elementos considerados para as sentenças.

Utilizado como ferramenta de avaliação de risco de reincidência criminal, para orientar decisões sobre sentenças e liberação de liberdade condicional, o algoritmo foi treinado a partir de um vasto banco de dados que inclui variáveis sociodemográficas, histórico de prisões e outros fatores, fornecendo uma pontuação de "risco" para os réus.

No entanto, estudos acadêmicos, como os conduzidos por Angwin et al. (2016), indicaram que o COMPAS exibia um viés racial ao classificar réus negros com pontuações de

risco mais elevadas do que réus brancos em situações similares. Isso ocorreu independentemente de histórico criminal objetivo ou de outros fatores que pudessem justificar essas diferenças de pontuação.

Os resultados acima apresentados provocaram debates acadêmicos e éticos sobre a confiabilidade e a justiça do COMPAS. Autores como Pasquale (2015) e Citron (2019) argumentam que os algoritmos de pontuação de risco perpetuam desigualdades sociais e raciais, desafiando princípios de igualdade e dignidade previstos na Constituição dos EUA, ao atribuir julgamentos com base em preconceitos históricos. Esse cenário agrava-se pela falta de transparência e pela dificuldade de contestar os critérios utilizados na pontuação.

Adentrando a temática, passa-se em revista o caso Loomis v. Wisconsin. Eric Loomis contestou a sentença recebida, argumentando que o uso do COMPAS violava seu direito ao devido processo, pois o algoritmo é um sistema pouco ou nada transparente. Essa característica impediu que a defesa avaliasse seu funcionamento interno e os dados usados para determinar a pontuação. Loomis alegou que o COMPAS havia influenciado sua sentença ao considerar variáveis ligadas a raça e gênero. A Suprema Corte de Wisconsin decidiu que o COMPAS poderia ser utilizado como “fator adicional” na decisão judicial, mas enfatizou a necessidade de cautela e de informar os juízes sobre as limitações do algoritmo (Bennett Moses e Chan, 2019).

Enfrentada a concretude do caso, a questão da transparência é um dos pontos centrais do debate acadêmico sobre o uso de ferramentas como o COMPAS. Wachter e Mittelstadt (2019) discutem a "opacidade algorítmica" e como ela limita o exercício dos direitos de defesa. Segundo os autores, a falta de transparência pode violar o devido processo, pois impede que os acusados compreendam como os fatores são ponderados nas decisões judiciais. O'Neil (2016) também critica algoritmos opacos, chamando-os de "armas de destruição matemática", que impactam negativamente minorias raciais e pessoas em situação de vulnerabilidade, o que reforça a necessidade de regulamentação.

Nos EUA, não há regulamentação federal específica para o uso de algoritmos no sistema judicial, mas a aplicação de IA deve respeitar princípios constitucionais, como o da Igualdade perante a Lei e o do Devido Processo, previstos na 14ª Emenda. A ausência de regulação permite interpretações controversas, e o uso de dados raciais acaba por institucionalizar discriminações (Citron, 2019).

Na superfície do objeto, a discriminação algorítmica representa uma ameaça direta aos direitos humanos, como os de igualdade e não discriminação. Trabalhos como o de Alexander (2012) colocam o COMPAS no contexto de discriminação racial sistêmica nos EUA, evidenciando que o sistema de justiça algorítmica muitas vezes reproduz desigualdades preexistentes.

Desta forma, o uso de algoritmos como o COMPAS representa um risco significativo à justiça e à imparcialidade. Há um consenso emergente na literatura sobre a necessidade de regulamentação, auditoria independente e transparência para mitigar vieses e proteger direitos constitucionais dos réus (Pasquale, 2015; Wachter e Mittelstadt, 2019). Portanto, a regulação no uso de algoritmos na justiça criminal é essencial para evitar que vieses resultem em injustiças e discriminação estrutural.

2. Reconhecimento Facial e a Polícia

Outro exemplo de violação de direitos humanos ocorre no uso de algoritmos de reconhecimento facial pelas forças policiais. Em 2020, Robert Williams, um homem negro, foi erroneamente identificado por um software de reconhecimento facial, resultando em sua prisão injusta. A detenção de Williams foi alvo de críticas de organizações de direitos civis, como a ACLU (American Civil Liberties Union), que argumentou que o uso dessa tecnologia ampliou a criminalização de minorias, evidenciando vieses raciais intrínsecos aos algoritmos. Embora as ações judiciais ainda estejam em andamento, o caso levantou discussões sobre a legalidade e ética do uso de IA para identificação criminal.

Este incidente, juntamente com outros, expôs os riscos de discriminação racial intrínsecos a esses sistemas e gerou um debate vigoroso entre legisladores, juízes e acadêmicos, que buscam equilibrar o uso dessas tecnologias com a proteção de direitos civis. Neste contexto, o trabalho de autores como Ruha Benjamin, Safiya Noble, e Virginia Eubanks contribui substancialmente para a discussão, reforçando as críticas já apontadas por outros doutrinadores, como Danielle Citron e Frank Pasquale.

O caso Williams chamou atenção para o viés racial nas tecnologias de reconhecimento facial, uma vez que, como diversos estudos indicam, esses algoritmos apresentam maior probabilidade de erro para rostos de indivíduos negros e de outras minorias (Buolamwini e Gebru, 2018). Esse viés já levou várias cidades americanas, como São Francisco, a proibir o

uso de reconhecimento facial por forças policiais, refletindo uma preocupação crescente com a proteção de direitos civis e com o cumprimento da Quarta e Décima Quarta Emendas (Green, 2019). No entanto, a ausência de uma legislação federal uniforme deixa essa questão em aberto, permitindo interpretações locais e estaduais que dificultam a criação de um padrão de respeito aos direitos constitucionais.

Além disso, a Suprema Corte dos Estados Unidos, embora ainda não tenha julgado diretamente a constitucionalidade do uso de reconhecimento facial no contexto criminal, possui precedentes, como o caso Katz v. United States (1967), que firmou o conceito de privacidade e proteção contra vigilância arbitrária, que vêm sendo utilizados para embasar decisões em tribunais inferiores. A invocação da Quarta Emenda, que protege a privacidade, e da Décima Quarta, que assegura igualdade perante a lei, aparece como base para legislações restritivas em algumas cidades e como argumento em tribunais que questionam o uso indiscriminado da tecnologia.

Ruha Benjamin, em sua obra Race After Technology (2019), argumenta que o desenvolvimento de algoritmos de reconhecimento facial e outras tecnologias de IA reflete um "racismo codificado", onde preconceitos históricos e sociais são reproduzidos e amplificados em novos sistemas digitais. Benjamin (2019) sustenta que o desenvolvimento desses algoritmos sem considerar as implicações raciais significa que práticas de discriminação, antes explícitas, agora são disfarçadas em decisões automatizadas, mas com o mesmo impacto social negativo. Ela defende que os direitos civis devem ser protegidos por meio de uma estrutura de responsabilização dos desenvolvedores e usuários dessas tecnologias.

A crítica de Benjamin (2019) é corroborada por Safiya Noble, que, em Algorithms of Oppression (2018), destaca como algoritmos podem perpetuar preconceitos e estigmas sociais, uma questão especialmente problemática quando esses sistemas são utilizados para fins policiais e judiciais. Noble (2018) adverte que o uso desses algoritmos cria um "efeito cascata de discriminação", no qual populações marginalizadas tornam-se alvo de vigilância e criminalização exacerbadas. Ela propõe uma regulamentação que envolva os próprios desenvolvedores, responsabilizando-os pela criação e implementação de algoritmos justos e transparentes.

Virginia Eubanks (2018), em seu trabalho Automating Inequality, acrescenta que as tecnologias de reconhecimento facial e outros algoritmos de predição representam uma nova

forma de exclusão digital, onde o acesso a oportunidades justas e a proteção de direitos civis são negados a grupos marginalizados. Para Eubanks (2018), os algoritmos se tornaram ferramentas de controle social, reproduzindo e agravando desigualdades estruturais ao classificar indivíduos como de "alto risco" com base em fatores socioeconômicos e raciais. Eubanks argumenta que o uso desses sistemas por instituições públicas viola o devido processo, uma vez que os algoritmos operam como "caixas-pretas", impossíveis de serem compreendidos ou contestados pelos afetados.

Frank Pasquale, em The Black Box Society (2015), defende que a opacidade dos algoritmos é uma ameaça aos direitos fundamentais, especialmente quando essas ferramentas são usadas para tomar decisões com consequências legais e sociais. Ele propõe um sistema de "responsabilidade algorítmica", que inclua auditorias independentes e uma legislação que exija transparência para algoritmos usados no setor público e na justiça criminal (Pasquale, 2015). Esta proposta ecoa nas ideias de Citron (2019), que alerta sobre os riscos de um estado de vigilância que pode levar à violação dos direitos de privacidade e igualdade, especialmente se a tecnologia é utilizada de maneira indiscriminada e sem a supervisão adequada.

Além disso, Buolamwini e Gebru (2018), em seu artigo "Gender Shades", fornecem uma análise crítica da precisão dos algoritmos de reconhecimento facial, especialmente em relação a minorias raciais e mulheres. O estudo de Buolamwini e Gebru (2018) foi fundamental para impulsionar mudanças regulatórias, ao demonstrar que o viés algorítmico não é apenas uma questão ética, mas também uma limitação técnica que compromete a validade e a confiabilidade das ferramentas utilizadas.

A análise dos autores revela que a implementação de tecnologias de reconhecimento facial e outros algoritmos de predição sem supervisão e regulamentação adequadas apresenta um risco significativo de violação dos direitos civis e humanos. Juristas e acadêmicos como Benjamin (2019), Noble (2018), Eubanks (2018), Citron (2019), e Pasquale (2015) defendem a criação de diretrizes legislativas rigorosas para garantir a transparência e a equidade no uso dessas tecnologias, de forma que elas não agravem as desigualdades já existentes.

Esses estudos apontam para a necessidade de uma regulamentação federal nos EUA que possa padronizar o uso desses algoritmos, assegurar a proteção dos direitos civis e minimizar os riscos de discriminação e vigilância desproporcional. Em última análise, a responsabilidade por garantir que o uso dessas tecnologias não viole os direitos humanos recai

sobre legisladores, desenvolvedores e o sistema judiciário, que devem atuar de forma conjunta para construir uma infraestrutura ética e transparente para o uso de IA no setor público.

3. Algoritmos de Crédito e o Direito à Igualdade

O uso de algoritmos de crédito por instituições financeiras para determinar a elegibilidade e taxas de crédito tem suscitado críticas e preocupações sobre a amplificação de desigualdades. Casos envolvendo empresas como Amazon e Apple, acusadas de discriminar mulheres na concessão de crédito, expõem a possibilidade de esses algoritmos replicarem vieses que levam à discriminação indireta.

A Equal Credit Opportunity Act (ECOA), lei estadunidense de 1974 que veda a discriminação baseada em características protegidas, tais como raça, cor, sexo, entre outras características, na obtenção de créditos e financiamento, ainda enfrenta desafios para garantir a igualdade quando aplicada a sistemas automatizados, dado que a opacidade dos algoritmos dificulta a comprovação de discriminação (Hurley e Adebayo, 2016).

O caso Apple Card de 2019, no qual limites de crédito mais baixos teriam sido concedidos a mulheres, e o caso Blass v. Wells Fargo, que acusou o banco de discriminar minorias raciais em empréstimos imobiliários, exemplificam a necessidade de regulamentação mais clara e mecanismos de transparência nos algoritmos de crédito. Para Frank Pasquale (2015), a "caixa-preta" dos algoritmos torna quase impossível a responsabilização e a prova de discriminação, sugerindo auditorias e transparência para garantir a aplicação da ECOA na era da inteligência artificial.

Para Solon Barocas e Andrew Selbst (2016), a discriminação indireta causada por variáveis correlacionadas a características protegidas, como o uso de proxies. Eles defendem o uso de regulamentações para limitar o uso dessas variáveis e exigir análise de impacto. Pauline Kim (2017) vai além, discutindo a “desigualdade algorítmica”, onde sistemas baseados em dados históricos perpetuam desigualdades preexistentes. Ela propõe que a ECOA abarque também a discriminação indireta, forçando instituições a demonstrar que seus algoritmos não impactam desproporcionalmente grupos vulneráveis.

Danielle Citron (2019) acrescenta que os algoritmos de crédito violam o direito à igualdade, garantido pela Décima Quarta Emenda dos EUA. Para Citron é necessário a

realização de uma interpretação judicial mais ampla, incluindo a discriminação indireta como violação de direitos civis.

Ainda, Ruha Benjamin (2019) critica o "racismo codificado" dos algoritmos e sugere uma abordagem de "responsabilidade antirracista" para que as empresas de tecnologia avaliem os impactos raciais de seus produtos.

Assim, é possível entendermos que há necessidade de reforma regulatória nos EUA para enfrentar a discriminação algorítmica. Com a necessidade de uma legislação robusta, com transparência, auditorias independentes e limitações ao uso de variáveis enviesadas, visando alinhar os princípios de igualdade ao contexto digital e garantir o uso ético e justo da tecnologia em decisões de crédito.

CONCLUSÃO

A análise dos casos apresentados revela que o uso de algoritmos no sistema de justiça e em outros setores críticos nos EUA pode resultar em decisões que violam os direitos humanos. A discriminação algorítmica se manifesta em vieses raciais, sociais e de gênero, prejudicando o direito à igualdade e à dignidade. Embora o sistema judicial estadunidense tenha reconhecido a existência de vieses em alguns casos, ele ainda enfrenta desafios na regulamentação eficaz dessas tecnologias, que continuam a afetar minorias e populações vulneráveis de forma desproporcional.

A atuação judicial e as medidas regulatórias adotadas até o momento são insuficientes para conter as práticas discriminatórias dos algoritmos. O desenvolvimento de políticas públicas que promovam a transparência e a responsabilização das empresas de tecnologia é fundamental para mitigar esses riscos. Além disso, a implementação de diretrizes éticas e auditorias independentes pode assegurar que algoritmos sejam treinados com dados representativos e imparciais, protegendo os direitos humanos de todos os indivíduos.

REFERÊNCIAS

ACLU. ACLU Sues Detroit Police Department for Misuse of Facial Recognition Technology. Disponível em: https://www.aclu.org/press-releases. Acesso em: 31 out. 2024.

ALEXANDER, Michelle. The New Jim Crow. Nova York: New Press, 2012.

AMERICAN CIVIL LIBERTIES UNION. Williams v. City of Detroit: face recognition false arrest. 2024. Disponível em: https://www.aclu.org/cases/williams-v-city-of-detroit-face-recognition-false-arrest. Acesso em: 28 nov. 2024.

ANGWIN, Julia; LARSON, Jeff; MATTU, Surya; KIRCHNER, Lauren. Machine Bias: There's software used across the country to predict future criminals. And it's biased against blacks. ProPublica, 2016. Disponível em: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing. Acesso em: 31 out. 2024.

BAROCAS, Solon; SELBST, Andrew D. Big Data's Disparate Impact. California Law Review, v. 104, p. 671-732, 2016.

BENJAMIN, Ruha. Race After Technology: Abolitionist Tools for the New Jim Code. Cambridge: Polity, 2019.

BENNETT MOSES, L.; CHAN, J. Algorithmic Bias in Criminal Justice Decision-Making. Cambridge Law Journal, v. 78, n. 1, p. 163-192, 2019.

BUOLAMWINI, Joy; GEBRU, Timnit. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. Proceedings of Machine Learning Research, v. 81, p. 77-91, 2018.

CITRON, Danielle Keats. Technology and Civil Rights: The Rise of a New Civil Rights Movement. Yale Law Journal, v. 128, n. 6, p. 2151-2204, 2019.

EUBANKS, Virginia. Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor. Nova York: St. Martin's Press, 2018.

GREEN, Jonathon. San Francisco Becomes the First City to Ban Facial Recognition Technology. Forbes, 2019.

HURLEY, Mikella; ADEBAYO, Julius. Credit Scoring in the Era of Big Data. Yale Journal of Law & Technology, v. 18, p. 148-216, 2016.

KIM, Pauline T. Data-Driven Discrimination at Work. William & Mary Law Review, v. 58, n. 3, p. 857-936, 2017.

NOBLE, Safiya Umoja. Algorithms of Oppression: How Search Engines Reinforce Racism. Nova York: NYU Press, 2018.

O'NEIL, Cathy. Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. Nova York: Crown, 2016.

PASQUALE, Frank. The Black Box Society: The Secret Algorithms That Control Money and Information. Cambridge: Harvard University Press, 2015.

WACHTER, Sandra; MITTELSTADT, Brent. A Right to Reasonable Inferences: Re-thinking Data Protection Law in the Age of Big Data and AI. Columbia Business Law Review, 2019.

WACHTER-BOETTCHER, Sarah. Technically Wrong: Sexist Apps, Biased Algorithms, and Other Threats of Toxic Tech. Nova York: W. W. Norton & Company, 2019.

7 Information Society and Law
FMU CENTRO UNIVERSITÁRIO

A INTELIGÊNCIA ARTIFICIAL E OS DIREITOS DAS PESSOAS E DO MEIO AMBIENTE: TECNOLOGIA, INOVAÇÃO, SUSTENTABILIDADE E EFETIVIDADE

ARTIFICIAL INTELLIGENCE AND THE RIGHTS OF PEOPLE AND THE ENVIRONMENT: TECHNOLOGY, INNOVATION, SUSTAINABILITY AND EFFECTIVENESS

Regina Vera Villas Bôas[1]; Tiago Cappi Janini[2]

"As leis não bastam, os lírios não nascem da lei"
(Carlos Drummond de Andrade)

Resumo: Trata-se de matéria atual e relevante, invocando reflexões sobre a Inteligência Artificial (IA), observada a partir das novas tecnologias, que se consolidam por inovações com repercussões na sustentabilidade. Os impactos da Inteligência Artificial (IA) geram consequências que podem (ou não) ofertar celeridade à efetividade dos Direitos. Em face da contemporânea crise global de defesa das garantias e direitos das pessoas, notadamente dos direitos fundamentais, a efetivação dos direitos, sejam eles privados ou públicos, individuais, coletivos e/ou difusos, cada vez se exibe mais distante. Também, a materialização da sustentabilidade, conclamada pelos Objetivos do Desenvolvimento Sustentável (ODS), dispostos pela Agenda 2030 da ONU, por meio de inovações trazidas pela Inteligência Artificial podem (ou não) salvaguardar a existência das gerações presente e futuras. A pesquisa é bibliográfica e documental, revisando legislações pertinentes, doutrina e jurisprudência, a partir de abordagem qualitativa de natureza básica e objetivo explicativo. Resultados parciais apontam incertezas quanto à efetividade dos direitos em face da crise global de defesa das garantias e direitos das pessoas - privados ou públicos, individuais, coletivos e/ou difusos -, notadamente dos direitos fundamentais, revelando de um lado distância e, de outro, proximidade, da materialização da sustentabilidade, almejada pelos Objetivos do Desenvolvimento Sustentável (ODS) - dispostos na Agenda 2030 da ONU -, na ambiência das inovações trazidas pela Inteligência Artificial, objetivando a salvaguarda a existência das gerações presente e futuras.
Palavras-Chave: Inteligência Artificial; Inovação; Sociedade da Informação; Efetividade dos Direitos; Sustentabilidade.

[1] Doutora em Direito das Relações Sociais (Direito Privado) e em Direitos Difusos e Coletivos pela Pontifícia Universidade Católica de São Paulo. Pós-Doutora em Democracia e Direitos Humanos pela Universidade de Coimbra (Ius Gentium Conimbrigae). Professora e pesquisadora do PG e PPG em Direito da PUC/SP, coord. do PP "Diálogo das Fontes: Efetividade dos Direitos, Sustentabilidade, Vulnerabilidades e Responsabilidades (PUC/SP). - email: revillasboas1954@gmail.com
CV: http://lattes.cnpq.br/4695452665454054 - https://orcid.org/0000-0002-3310-4274
[2] Doutor em Direito do Estado (Tributário) pela PUC/SP. Professor e pesquisador do Programa de Mestrado em Direito da Sociedade da Informação da FMU e na graduação em Direito da FMU. Estágio Pós-Doutorado (PNPD-CAPES) na Universidade Estadual do Norte do Paraná (UENP).

Abstract: This is a current and relevant matter, invoking reflections on Artificial Intelligence (AI), observed from new technologies, which are consolidated by innovations with repercussions on sustainability. The impacts of Artificial Intelligence (AI) generate consequences that may (or may not) speed up the effectiveness of Rights. In the face of the contemporary global crisis in the defense of people's guarantees and rights, notably fundamental rights, the realization of rights, whether private or public, individual, collective and/or diffuse, is increasingly distant. Also, the materialization of sustainability, called for by the Sustainable Development Goals (SDGs), set forth by the UN 2030 Agenda, through innovations brought by Artificial Intelligence may (or may not) safeguard the existence of present and future generations. The research is bibliographic and documentary, reviewing pertinent legislation, doctrine and jurisprudence, from a qualitative approach of a basic nature and explanatory objective. Partial results point to uncertainties regarding the effectiveness of rights in the face of the global crisis in the defense of people's guarantees and rights - private or public, individual, collective and/or diffuse - notably fundamental rights, revealing, on the one hand, distance and, on the other, proximity, from the materialization of sustainability, desired by the Sustainable Development Goals (SDGs) - set forth in the UN 2030 Agenda -, in the ambience of innovations brought by Artificial Intelligence, aiming to safeguard the existence of present and future generations.
Keywords: Artificial Intelligence; Innovation; Information Society; Effectiveness of Rights; Sustainability.

INTRODUÇÃO

As reflexões sobre a Inteligência Artificial reportam o pesquisador à sociedade da informação e, consequentemente, à necessidade de ampliação do conhecimento dos conceitos e fundamentos relacionados à tecnologia, à inovação e à evolução da informação, entre outros, que exibem as novas realidades do presente século.

Byung-Chul Han, na obra publicada pela editora Vozes, em 2019 (Hiperculturalidade: Cultura e Globalização) argumenta sobre a superficialidade presente nas relações da sociedade contemporânea, baseadas nas conexões digitais, que se apresentam fluidas, sem possibilidade de raízes fixadas e se pautam pela ausência de verticalidade e de compromissos sólidos. Presente, atualmente, na identidade da pessoa, uma fragmentação que tem origem nos impactos causados pela sua necessidade de estar, diuturnamente conectada e em evidência nas redes sociais. Essa conexão instantânea afasta, atualmente, a presença do amor verdadeiro, uma vez que demandam tempo e dedicação, difíceis de se concretizarem, na contemporaneidade. A superficialidade das conexões implicam educação e aprendizado rasos e superficiais, que não permitem aprofundamentos das informações e do conhecimento transferidos, os quais seguem, assim, fragmentados, marcando a busca da valorização do tempo e das reflexões atinentes à

promoção de envolvimentos verticalizados e significativos atinentes aos objetos de apreciação do homem.

Os sintomas da sociedade contemporânea se exibem como frutos de realidades supérfuas, difusas, distantes de situações de concretudes e de reflexões na busca do conhecimento, frutos estes, observados e assimilados tanto pelas pessoas "per se", coletividades de pessoas, empresas, setores públicos e privados e mercados, entre outros.

Conceitos novos são trazidos à nova ambiência, passando a ser assimilados e desenvolvidos globalmente, por sociedades e respectivos mercados, como é o caso do "mundo VUCA", que concerne às incertezas, à celeridade e às novidades oriundas das rápidas tranformações por eles experimentadas. Essa realidade ocorre a partir da década de 1990, marcada pelo distanciamento de fortes polarizações, até então, presentes, nos estados americanos.

A presente pesquisa, nesse contexto social e das novas tecnologias, objetiva refletir sobre a Inteligência Artificial (IA), que vem se consolidando a partir de inovações com repercussões na sustentabilidade, recordando que os impactos da Inteligência Artificial (IA) geram consequências que podem ofertarr maior ou menor efetividade aos Direitos.

Existe uma crise global no cumprimento das garantias e direitos das pessoas, distanciando, cada vez mais, a efetivação desses direitos, sejam eles privados ou públicos, individuais, coletivos e/ou difusos. Também, a materialização da sustentabilidade, conclamada pelos Objetivos do Desenvolvimento Sustentável (ODS), dispostos pela Agenda 2030 da ONU, podem (ou não) salvaguardar a existência das gerações presente e futuras, a partir das inovações trazidas pela Inteligência Artificial.

A metodologia utilizada na presente pesquisa se vale do método das referências bibliográficas e documental, revisando legislações pertinentes, doutrina e jurisprudência, a partir de abordagem qualitativa de natureza básica e objetivo explicativo.

Os estudos apresentam resultados parciais apontando incertezas relacionadas à efetividade dos direitos em face da crise global de defesa das garantias e direitos das pessoas, notadamente dos direitos fundamentais, revelando de um lado distância e, de outro, proximidade, da materialização da sustentabilidade, almejada pelos Objetivos do Desenvolvimento Sustentável (ODS) da Agenda 2030 da ONU, na ambiência das inovações trazidas pela Inteligência Artificial, objetivando a salvaguarda a existência das gerações presente e futuras.

Por derradeiro, os estudos contribuem para a promoção do conhecimento, ofertando reflexões sobre a sociedade de informação, a inovação, a Inteligência Artificial (IA) e as consequências que essas novas realidades e conceitos podem trazer à concretude dos direitos e materialização da sustentabilidade, conclamada pelos Objetivos do Desenvolvimento Sustentável (ODS), dispostos na Agenda 2030 da ONU, na salvaguarda das gerações presente e futuras.

1 O MUNDO "VUCA", A INTELIGÊNCIA ARTIFICIAL, A EFETIVIDADE DOS DIREITOS E A SUSTENTABILIDADE

Entre os conceitos novos trazidos pela sociedade da informação, imiscuidos nos mercados e ambiências vividas pelo homem, tem-se o "mundo VUCA", cuja sigla identifica situações de incerteza, complexidade, difusidade, ambiguidade e novidade, oriundas das rápidas tranformações trazidas pela contemporaneidade. Entender esse mundo "VUCA" requer o conhecimento de variadas realidades, atinentes à tecnologia, às mudanças tecnológicas e às condutas das pessoas, notadamente dos consumidores dos mercados, os quais alcançados pelas novas tecnologias são desafiados pelo enorme volume de novidades, conceitos e transformações das sociedades e mercados, refletidos diretamente nos seus comportamentos.

Mas, o que, de fato, significa esse vocábulo ou sigla "VUCA"?

O vocábulo "VUCA" designa uma sigla, que na língua inglesa é explicada por cada letra que compõe referida sigla. A letra "*V*" (*Volatility*) se explica pela "volatilidade", implicando as mudanças céleres, episódicas, extemporâneas, imprevisíveis ocorridas nos ambientes; a letra "*U*" (*Uncertainty*) pela "incerteza" designando a ausência de previsibilidade, da limitação da capacidade de previsão dos impactos no ambiente, exigindo muito preparo e flexibilidade das instituições no enfrentamento das imprevisões e incertezas no ambiente; a "*C*" (*Complexity*) pela "complexidade" de realidades, elementos e fatores multifacetados, que, apesar de poderem ser exibidos em realidades dialógicas, implicam relações de causa e efeito de difíceis entendimentos, e exigem a consideração de variáveis interdependentes nas soluções dos problemas apresentados; a letra "*A*" (*Ambiguity*) pela "ambiguidade" designando uma imprecisão, obscuridade, falta de clareza e nitidez sobre o significado dos eventos, apontando informações incompletas, difusas e/ou contraditórias, tornando difíceis tomadas claras de decisões e desenvolvimento de capacidade de operar a partir de informações imprecisas e interpretações de distintos significados,

em um mesmo contexto.

A volatilidade, a incerteza, a complexidade e a ambiguidade implicam situações/estados vividos globalmente pelas sociedades e mercados que enfrentam enormes e céleres transformações, as quais influenciam instituições de inúmeras e variadas ordens, poderes, governos, organizações, pessoas físicas e jurídicas, indistintamente.

Assim, os estados da volatilidade (*volatility*), incerteza (*uncertainty*), complexidade (*complexity*) e ambiguidade (*ambiguity*) desafiam o conhecimento de elementos da tecnologia e das transformações tecnológicas que implicam diretamente mudanças das condutas dos consumidores e dos mercados, alcançados pelas novas tecnologias, desafiadoras do conhecimento das novidades e dos conceitos que os influenciam.

Nesse contexto de modificações tecnológicas, a temática da Inteligência Artificial (IA), inserida na "sociedade da informação", se revela como uma das maiores transformações tecnológicas do presente século – uma mudança paradigmática – desafiando disciplinas e situações jurídicas, a exemplo da tutela de proteção da dignidade da pessoa humana, do papel desempenhado pelos algoritmos no Poder Judiciário e em face de discriminações e violações de direitos humanos, além dos impactos nas relações privadas, públicas, individuais, coletivas e/ou difusas, e da responsabilidade e proteção de dados nos sistemas de agilização da produção, desafiados por uma ética própria dos mecanismos da Inteligência Artificial (IA).

Os estudos, de um lado, revelam que a Inteligência Artificial (IA) corrobora a otimização das atividades e tarefas jurídicas cotidianas, entre as quais: a leitura inicial e/ou revisional de inúmeros e variados documentos, destrinchando e identificação alguns parâmetros e padrões sobre a matéria apreciada, auxiliando e ofertando celeridade à compreensão do conteúdo dos documentos oferecido à leitura dos instrumentos da Inteligência Artificial (IA)[3].

De outro lado, a Inteligência Artificial (IA) acelera os sintomas de ansiedade, insegurança e difusidade que desafiam, globalmente, as pessoas e as coletividades, cada vez mais inseguras, incertas e resilientes, além das sociedades, cada vez mais fluidas, líquidas e complexas, enfrentando céleres transformações socioambientais.

[3] **FASOLO**, Lucas de A. S. Dalbem. A relação e os impactos da IA no Direito. Disponível em > https://www.jusbrasil.com.br/artigos/a-relacao-e-os-impactos-da-ia-no-direito/1804866246#:~:text=A%20IA%20pode%20ajudar%20a,advogados%20tomem%20decis%C3%B5es%20mais%20informadas. Acesso em > 24/OUT/2024.

Afirma Cartaxo[4], a esse respeito, que o direito se relaciona com "um grande volume de dados e diversos tipos de documentação a serem analisados. Com a automação das tarefas jurídicas, cada vez mais o profissional jurídico pode poupar tempo em relação a essa quantidade de informações". Destaca que a inteligência artificial pode "reduzir o tempo necessário à revisão de documentos em até 60%, transformando a eficiência operacional dos escritórios de advocacia", reduzindo tempo e aumentando a precisão ao identificar padrões e cláusulas relevantes em grandes conjuntos de dados. Traz o exemplo do software "Lex Machina" que avalia dados que conseguem prever tendências e resultados de conflitos, corroborando o trabalho advocatícios na formulação de estratégicas, além de que referidos mecanismos, apresentam plataformas que têm alcançado percentuais de precisão das suas previsões, em torno de 70%. Assevera o avanço exponencial da tecnologia, trazendo relatório da Empresa Thomson Reuters, de 2021, com a informação de que "50% dos escritórios de advocacia nos Estados Unidos estão utilizando alguma forma de tecnologia de IA" marcando, assim, significativa evolução na aceitação da automatização; e que estudo do McKinsey Global Institute, de 2019, avalia que "23% das tarefas realizadas por advogados podem ser automatizadas com as tecnologias existentes", apontando o enorme potencial de crescimento e transformação no setor.

Arremata Cartaxo[5] afirmando que a alfabetização tecnológica dos operadores do direito será essencial à prática da profissão, e revela a necessidade da existência de "regulamentações mais rigorosas e transparência nos algoritmos utilizados na garantia de uma justiça verdadeiramente imparcial e justa". Lembra que a União Europeia, atualmente, lidera a realidade com um regulamento de Inteligência Artificial (IA), objetivando o estabelecimento de padrões éticos à utilização adequada da inteligência tecnológica; e que para democratizar o acesso a serviços, antes financeiramente inacessíveis para muitos, "startups de legaltech" desenvolvem, até gratuitamente, sistemas de consultoria jurídica àqueles que aferem baixas rendas.

[4]CARTAXO, Mac Amaral. O impacto da inteligência artificial na prática jurídica. Disponível em> https://www.conjur.com.br/2024-mai-10/o-impacto-da-inteligencia-artificial-na-pratica-juridica/ Acesso em > 26/OUT/2024.
[5]CARTAXO, Mac Amaral. O impacto da inteligência artificial na prática jurídica. Disponível em> https://www.conjur.com.br/2024-mai-10/o-impacto-da-inteligencia-artificial-na-pratica-juridica/ Acesso em > 26/OUT/2024.

Na esteira da afirmação de Cartacho[6], a automação das tarefas por meio da Inteligência Artificial (IA) pode diminuir a necessidade do trabalho humano, quando tratar-se de tarefas repetitivas, implicando insegurança na manutenção dos empregos. Todavia, também, libera os profissionais, concedendo-lhes mais tempo para lidarem com outras tarefas mais complexas, corroborando o potencial de valoração e qualidade dos serviços realizados.

Nesse sentido, os estudos apontam incertezas relacionadas à efetividade dos direitos, diante da crise global de defesa dos direitos das pessoas, do meio ambiente, e da materialização da sustentabilidade, invocada pelos 17 Objetivos do Desenvolvimento Sustentável (ODS), proclamados pela Agenda 2030 da ONU, no ambiente das inovações trazidas pela Inteligência Artificial, objetivando salvaguardar a existência das gerações presente e futuras. Apontam, também, contribuições à promoção do conhecimento, ao ofertar reflexões sobre a sociedade de informação, a inovação, a Inteligência Artificial.

CONCLUSÃO

Os presentes estudos, no contexto da sociedade da informação e das novas tecnologias, objetivam refletir sobre a importância da Inteligência Artificial (IA), que vem se consolidando com repercussões nos direitos, no meio ambiente e na materialização da sustentabilidade. Revelam a enorme crise global no cumprimento dos direitos que, cada vez mais, deixam de ser efetivados, além da sustentabilidade conclamada pelos Objetivos do Desenvolvimento Sustentável (ODS), dispostos pela Agenda 2030 da ONU, que almejam salvaguardar a existência das gerações presente e futuras, a partir das inovações trazidas pela Inteligência Artificial (ou não).

Valendo-se do método das referências bibliográficas e documental, revisando legislações pertinentes, doutrina e jurisprudência, a partir de abordagem qualitativa de natureza básica e objetivo explicativo, os estudos apontam incertezas quanto à concretude dos direitos em face da crise global de defesa dos direitos, notadamente dos fundamentais. Revela distância, ou proximidade, na efetividade da sustentabilidade proclamada pelos 17 Objetivos do Desenvolvimento Sustentável (ODS) da Agenda 2030 da ONU, no ambiente das inovações, oriundas da Inteligência Artificial, objetivando a existência intergeracional.

[6] CARTAXO, Mac Amaral. O impacto da inteligência artificial na prática jurídica. Disponível em> https://www.conjur.com.br/2024-mai-10/o-impacto-da-inteligencia-artificial-na-pratica-juridica/ Acesso em > 26/OUT/2024.

As mudanças paradigmáticas são prenunciadas pela sociedade da informação e anunciadas com a chegada da Inteligência Artificial (IA), esta designando uma nova tecnologia que surge tendo entre os seus objetivos, para viabilizar a capacidade e o aprendizado sobre máquinas que materializam atividades e tarefas complexas, propiciando celeridade das análises de dados e tomadas de decisões, de maneira a potencializar e promover transformações de governos, empresas, e outros âmbitos e dimensões sociais, a exemplo da economia, da política, do direito.

Os estudos reforçam o antagonismo das visões sobre a realidade da Inteligência Artificial (IA). No mundo jurídico, por exemplo, uma das visões atine às vantagens conquistadas pela eficiente realização das atividades jurídicas, entre outras, a automatização de tarefas rotineiras, a leitura e revisão de documentos feitas pelos operadores do direito - desde uma simples pesquisa doutrinária e/ou jurisprudencial e/ou legislativa, até inúmeras e complexas estratégias de promoção da justiça e identificação de padrões nos conjuntos dos dados investigados - o que corrobora uma melhor elaboração de petições, pareceres e decisões jurídicas. Também, o tempo recorde propiciado pela Inteligência Artificial (IA), na apreciação de idêntica quantidade de documentos, permitindo aos operadores do direito utilizarem, em outras tarefas ou ativiades jurídicas, o tempo economizado com a utilização da Inteligência Artificial (IA)".

A Inteligência Artificial (IA) oferta alguns desafios ao mundo jurídico, entre os quais a incerteza, a insegurança e a desconfiança atinentes aos resultados obtidos nas pesquisas orientadas pela Inteligência Artificial (IA", cuja produção dos textos se torna automática, a partir dos comandos feitos pelo homem. Isso implica a necessidade de comandos precisos, completos e bem elaborados na alimentação dos mecanismos da Inteligência Artificial (IA). A busca de resultados "confiáveis", por meio da Inteligência Artificial (IA), exigem, também, a alimentação de dados confiáveis, eis que, ao contrário, qual seja, a alimentação de dados tendenciosos, produzia, certamente, resultados tendenciosos; a alimentação de dados desprovidos de valores éticos, também produziria resultados que desprestigiariam referidos valores.

A Inteligência Artificial (IA) é uma tecnologia poderosa, que deve ser utilizada de maneira cuidadosa, a partir de objetivos claros e pontuais, de valores éticos que embebem a base e fundamentam a estrutura de apoio dos operadores dos mecanismos, fatos estes que,

expressos com dubiedade (mesmo que implicitamente), podem provocar situações de injustiça, a partir de decisões de discriminação e/ou contrárias à legislação, desafiando situações de responsabilidade jurídica pelo pagamento de indenizações por danos e/ou lesões provocados pela Inteligência Artificial (IA).

Apesar dos desafios relacionados à confiabilidade dos resultados, os estudos revelam que a Inteligência Artificial (IA) pode transformar realidades, inclusive a jurídica, oferecendo eficiência, celeridade e maneiras de atuação estratégica, objetivando uma compreensão mais clara e singela das complexidades, de maneira de ofertar disponibilidade de tempo aos operadores jurídicos, enquanto ela (IA), realiza tarefas, normalmente mais demoradas e detalhadas, no lugar desses operadores. Pode, também, extrair padrões de conjuntos de dados apreciados, além de antecipar alguns resultados de problemas propostos em tempo recorde, em face do desempenho cotidiano do homem.

Por derradeiro, os estudos contribuem à promoção do conhecimento, fornecendo reflexões sobre a sociedade de informação, a Inteligência Artificial (IA), a inovação, e as consequências que referidas realidades e conceitos, em tese, podem trazer à efetividade dos direitos e à concretização da sustentabilidade, invocada pelos 17 Objetivos do Desenvolvimento Sustentável (ODS), da Agenda 2030 da ONU, na salvaguarda intergeracional.

REFERÊNCIAS

ANDRADE, Carlos Drummond. Nosso tempo. Disponível em https://www.letras.mus.br/carlos-drummond-de-andrade/881736/. Acesso em: 27 out. 2024.

CARTAXO, Mac Amaral. O impacto da inteligência artificial na prática jurídica. Disponível em: https://www.conjur.com.br/2024-mai-10/o-impacto-da-inteligencia-artificial-na-pratica-juridica/. Acesso em: 26 out. 2024.

FASOLO, Lucas de A. S. Dalbem. A relação e os impactos da IA no Direito. Disponível em: https://www.jusbrasil.com.br/artigos/a-relacao-e-os-impactos-da-ia-no-direito/1804866246#:~:text=A%20IA%20pode%20ajudar%20a,advogados%20tomem%20decis%C3%B5es%20mais%20informadas. Acesso em: 24 out. 2024.

HAN, Byung-Chul. **Hiperculturalidade**: Cultura e Globalização. Tradução de Gabriel Salvi Philipson. Petrópolis, RJ: Vozes, 2019.

SILVA, Douglas da. O que é Mundo VUCA? Conheça o conceito e como lidar com essa realidade.**Web Content & SEO Associate**, LATAM. Atualizado em 9 março 2022.

Disponível em: https://www.zendesk.com.br/blog/o-que-e-mundo-vuca/. Acesso em: 23 out. 2024.

VILLAS BÔAS, Regina Vera. Contemporaneidade e efetividade dos direitos fundamentais sociais constitucionais no ordenamento jurídico nacional. **Revista Jurídica Unicuritiba**, v. 3, nº 75, 2023.

7 Information Society and Law
FMU CENTRO UNIVERSITÁRIO

INTELIGÊNCIA ARTIFICIAL E O IMPACTO NAS RELAÇÕES DE TRABALHO

ARTIFICIAL INTELLIGENCE AND THE IMPACT ON WORK RELATIONS

Selma Strublic[1]

Resumo: O estudo apresenta uma síntese sobre as relações de trabalho ao longo da história até os dias atuais com destaque ao crescente uso de tecnologias, ferramentas informatizadas e aplicações com uso de inteligência artificial (IA). Tem por objetivo destacar aspectos favoráveis e desfavoráveis do uso IA na relação de emprego e no comportamento dos empregados e empregadores. Além de uma breve pesquisa bibliográfica, o artigo aponta assuntos em pauta no Poder Legislativo, com a tramitação de um projeto de lei sobre a matéria; e, no Poder Judiciário com o julgamento em curso de um recurso extraordinário concernente a relação de emprego.
Palavras-Chave: Emprego; Inteligência Artificial; Relação de Trabalho; Riscos; Tecnologia.

Abstract: The study summarises work relationships throughout history to the present day, highlighting the growing use of technologies, computerized tools and applications based on artificial intelligence (AI). It aims to underline favourable and unfavourable aspects of using AI in the employment relationship and the behaviour of employees and employers. In addition to brief bibliographical research, the article highlights issues on the agenda in the legislative branch, with the processing of a bill on the matter; and, in the judiciary with the ongoing trial of an extraordinary appeal concerning the employment relationship.
Keywords: Employment; Artificial Intelligence; Employment Relationship; Risks; Technology.

INTRODUÇÃO

Algumas instituições vêm realizando pesquisas periódicas e cada vez mais aperfeiçoadas sobre os impactos dos modelos de inteligência artificial (IA) na relação de trabalho. Não seria imponderado simplificar que a preocupação humana em relação aos seus futuros produtivos e de sustento é cada vez mais evidenciado em tais pesquisas. E esse não é um assunto novo. Proporcionalmente, nossos ancestrais vivenciaram os mesmos receios desde a Primeira Revolução Industrial, em meados do século XVII. Toda automação e toda mudança,

[1] Graduada em Arquitetura e Urbanismo pela Universidade São Judas Tadeu - SP. Pós-Graduada em Engenharia de Transporte pela Escola de Engenharia de São Carlos da Universidade de São Paulo (USP). Pós-Graduada em Gestão Econômica e Estratégica de Projetos (MBA) pela Fundação Getúlio Vargas - SP. Graduanda em Direito pelo Centro Universitário das Faculdades Metropolitanas Unidas (FMU).

naturalmente, causam desconfortos nas rotinas de vida de todos os seres humanos, dos mais abastados aos mais humildes.

A distinção no atual momento é que o impacto nas relações de trabalho está acontecendo mais rapidamente, sem muita possibilidade de manobra ou mitigação que possibilitasse um planejamento para médio prazo. O prazo é hoje. Diariamente algumas funções deixam de existir graças a um avanço tecnológico que garante mais eficiência no processo produtivo, menor incidência de erros, economia com salários e infraestrutura empresarial.

Os discursos acadêmicos têm exercido o papel de estímulo a estudos focados em áreas de conhecimento mais complexas, responsáveis pela retaguarda e desenvolvimento da Inteligência Artificial. Mas, como fica a grande massa da população, cujas competências profissionais limitam-se à realização de atividades braçais, que figuram no topo da lista das dispensáveis pela IA? O fomento à empregabilidade precisa de alguns ajustes consistentes para dar conta da realidade das relações de trabalho no Brasil.

O Relatório Anual 2024 do FMI – Resiliência Diante da Mudança – indica que "cerca de 60% dos empregos nas economias avançadas podem ser afetados pela inteligência artificial[2]". Já em países de baixa renda o índice deve ser de 26%. Considerando que o Brasil está na lista das 10 maiores economias mundiais, o índice de 60% levantado pelo FMI (Fundo Monetário Internacional) é bastante preocupante em termos de mercado de trabalho não só para os mais de 7 milhões de desempregados[3], de acordo com o IBGE, mas também para àqueles que estão em atividades suscetíveis de serem substituídas pela IA.

Posto isso, o objetivo desta breve pesquisa consiste em trazer um relato histórico das relações de trabalho e um panorama do momento atual, com seus impactos e preocupações em relação ao futuro do emprego. No item 2 são tratadas algumas tecnologias atualmente em voga e os reflexos na relação de emprego e na judicialização. Em continuidade são apresentadas diferentes aplicações da IA, seus riscos e suas oportunidades.

[2] Relatório Anual do FMI 2024. Disponível em <https://cdn.sanity.io/files/yg4ck731/production/54d1dcaff44e0086c5be9844c78fa54b995c5445.pdf/Portuguese%202024%20IMF%20Annual%20Report.pdf>. Acesso em 20.out.2024.

[3] IBGE – Instituto Brasileiro de Geografia e Estatística. Disponível em <https://www.ibge.gov.br/explica/desemprego.php>. Acesso em 20.out.2024.

1 EVOLUÇÃO DAS RELAÇÕES DE TRABALHO NO BRASIL

Nunca é demais destacar que – genericamente – o empregador formou-se, cresceu e enriqueceu à custa do necessitado. Para conter os abusos, diversas frentes atuaram no sentido de delinear os limites das relações e das obrigações e deveres das partes, com destaque aos movimentos sociais, leis de proteção aos trabalhadores, reconhecimento do direito à greve, instituição de sindicatos, entre outros. Até que as grandes guerras interromperam os avanços e uma vida normal só pôde ser retomada após 1945, impulsionada pelas reconstruções pós-guerra. Mas a normalidade já não era a mesma, pois o anseio por condições dignas prevaleceu em diversos pleitos, ações sindicais e lutas dos empregados. Como resultado, depois de muita violência e sacrifícios, destacaram-se os salários melhores, estipulação de benefícios e melhorias nos locais de trabalho.

No Brasil a história não é tão simples, visto que além das necessidades empregatícias o país viveu períodos monárquico, ditatorial, conservador e – quase sempre – cerceador de direitos que também refletiram nas relações de trabalho. Ainda que em 1941 tenha sido criada a Justiça do Trabalho, durante o governo de Getúlio Vargas, a Consolidação das Leis Trabalhistas, por meio do Decreto-Lei nº 5.452/1943, foi sancionada carecendo de reformas objetivas nas relações de trabalho. Esperava-se que o próprio governo promovesse tais reformas, mas o afastamento de Getúlio Vargas do poder adiou os anseios trabalhistas. Absurdamente, vivenciamos interrupções de greves em 1968 com o uso de tanques de guerra requisitados pelo próprio Ministro do Trabalho da época.

Algum alento trouxe a Constituição Federal de 1988, denominada de Constituição Cidadã, justamente por incorporar as conquistas das lutas das décadas de 1960 e 1970. Além dos Direitos e Garantias Fundamentais do art. 5º da CRFB/88, o Capítulo II traz nos arts. 6º a 11 os Direitos Sociais e dos Trabalhadores, com proteções de eficácias plenas.

Depois disso, alguns fatos marcaram mudanças expressivas nas relações de trabalho como a abertura econômica e liberação das importações na década de 1990, promovidos pelo presidente Fernando Collor. Em 2019, observamos a extinção do Ministério do Trabalho pelo presidente Jair Bolsonaro. Em meados de 2021, o Ministério foi oficialmente recriado.

Ao longo da história, fica evidenciado que a marca mais significativa diz respeito à fragilidade na efetivação de direito dos empregados. Ainda que muito tenha evoluído em termos tecnológicos, este não foi o protagonista das reinvindicações, pois a pretensão pelo básico era

(ou ainda é!) primaz. Muito antes do empregado se interessar por uma nova ferramenta que possa agilizar sua atividade, ele precisa efetivamente ter emprego, ser remunerado devidamente e com condições dignas. Talvez isso explique os motivos da IA ainda ser assunto restrito de determinados segmentos profissionais.

2 AVANÇOS TECNOLÓGICOS NAS ATIVIDADES PRODUTIVAS

É natural que as relações de trabalho ocorram em consonância com as particularidades da localidade e das conjunturas sociais e políticas do país. Por isso, é tão inadequado apropriar-se de pesquisas sobre o uso das tecnologias e da inteligência artificial desenvolvidas na Europa ou nos Estados Unidos na realidade de indústrias e serviços instalados fora das principais capitais brasileiras. E até mesmo nas capitais.

O ímpeto de certos setores em alcançar equiparação internacional para fins competitivos – e dada a singularidade do profissional empenhado nesse tipo de atividade – admite estipulações na relação de trabalho diferenciadas para o hipersuficiente, amparada na própria legislação brasileira (art. 444 da CLT), ou seja, aquele portador de diploma de nível superior e que perceba salário mensal igual ou superior a duas vezes o limite máximo dos benefícios do Regime Geral de Previdência Social. Isso representa algo em torno de R$ 16 mil, sendo um salário relativamente normal quando se trata de profissionais dos segmentos de TI. E um salário quase utópico para os mais de 80% da população brasileira que estão classificados nas Classes C, D e E, de acordo com o IBGE (Instituto Brasileiro de Geografia e Estatística). De qualquer forma, aqueles profissionais, pertencentes a classes com renda entre 5 e 15 salários-mínimos, podem se valer das tendências internacionais que utilizam IA e realizar tratativas diferenciadas em suas relações com empregadores. Aqui, uma solução tecnológica é vista como um alívio, uma inovação para potencializar suas rotinas, para abrir espaço para novas empreitadas e permitir alavancar patamares gerenciais e diretivos: a IA contribuindo positivamente para que esse profissional não fique estagnado.

Retomando, temos uma fotografia não tão radiante em outros segmentos e tipos de profissionais. Por uma série de fatores, inclusive por força do período da pandemia da Covid-19, muitos setores foram reduzidos e até mesmo eliminados. É o caso do telemarketing, cujo início data da década de 1970, mas que expandiu significativamente no início dos anos 2000. Porém hoje vem gradativamente sendo ‘engolido’ pela tecnologia, com sistemas robotizados de

atendimento ao cliente e de oferta de serviços. A avalanche de ligações diárias também perdeu forças e motivou a adaptação de sérias empresas para evitar rejeição ao invés de satisfazer as necessidades dos clientes. Outro fator representativo na redução do quadro de profissionais das empresas de telemarketing está relacionado aos próprios entraves da relação de trabalho, uma vez que concentrar mais de 100 pessoas num mesmo espaço, no mesmo turno de trabalho, garantindo benefícios e condições dignas e amistosas de relacionamento mostra-se relativamente mais oneroso que investir em sistemas informatizados. Infelizmente, o pensamento empresarial privilegia o lucro e não os direitos sociais.

A consequência do exemplo do telemarketing é o desemprego, pois o profissional menos capacitado ou sem formação técnica dificilmente obtém realocação em outros setores. Investimentos em capacitação, entre tantos benefícios, apoiam a recondução a segmentos que exigem qualificações menos braçais ou mais intelectualizadas.

Em contrapartida, o desemprego aliado a IA mudou a concepção do transporte individual. Exemplo clássico, amplamente tratado tanto judicialmente como academicamente, é a Uber. Inicialmente, a plataforma desenvolvida pela gigante americana visava trazer uma opção ao taxi, mas o sucesso (e também as polêmicas) foi tão surpreendente que a concorrência logo surgiu para repartir uma fatia desse mercado. Uma pesquisa divulgada em abril de 2023 na imprensa indica que mais de 1,6 milhão de pessoas trabalham como motoristas ou entregadores de aplicativos.

Tal como a fábula dos dois ratinhos que caíram no balde de leite e que só sobrevive quem se mexe, a Uber vem investindo cada vez mais em tecnologias e inovações em inteligência artificial para criar algoritmos avançados de otimização de rotas, análise das preferências e comportamentos dos usuários, redução nos tempos de espera e eficiência dos motoristas.

As polêmicas envolvendo a Uber, não restritas ao Brasil, residem justamente na relação de trabalho entre a plataforma e os motoristas. Caracteriza-se ou não o vínculo empregatício? O RE 1446336 que tramita no STF desde junho de 2023, encaminhado para análise do Ministro Edson Fachin em agosto de 2024, trata, "à luz dos artigos 1º, IV; 5º, II, XIII; e 170, IV da CRFB/88, da possibilidade do reconhecimento de vínculo de emprego entre motorista de aplicativo de prestação de serviços de transporte e a empresa criadora e

administradora da plataforma digital intermediadora”[4]. Interessante a leitura do destaque abaixo, retirado do Inteiro Teor do Acórdão, publicado em julho de 2024:

> Nesse sentido, a 8ª Turma do Tribunal Superior do Trabalho consignou que: i) a Uber é uma empresa prestadora de transporte e, não, uma plataforma digital; ii) a Uber fixa o preço da corrida, sem nenhuma ingerência do motorista prestador; iii) a Uber realiza o cadastramento, delimitando exigências mínimas, aceitando ou rejeitando o motorista; iv) a Uber é quem fixa o percentual da empresa a ser descontado; v) **o motorista não possui nenhum tipo de controle em relação ao preço das corridas**; vi) a única **autonomia do motorista restringe-se a definir horários** e aceitar ou recusar as corridas; vii) a Uber efetua unilateralmente o desligamento do motorista, caso ele descumpra alguma norma interna; viii) o motorista não possui autonomia para escolher clientes, mas, tão-somente, corridas; e, por fim, ix) a **subordinação jurídica se caracteriza pelos meios telemáticos e informatizados de controle** (parágrafo único do art. 6º da CLT), o que afastaria qualquer tese relacionada à atividade-fim ou subordinação objetiva/estrutural (eDOC 36). (g.n.).

Observa-se a posição do relator quanto a um dos elementos que caracterizam a relação de trabalho, isto é, a subordinação. Mas essa subordinação, tal qual caracterizado na CLT, distingue-se do modelo tradicional de empregado lotado numa planta produtiva. São múltiplas as formas de prestar serviços nos dias atuais: presencial, teletrabalho, intermitente, temporário, terceirizado, empreitada, contrato PJ, parcial, entre outros até mesmo desconhecidos, mas que suprem as expectativas do empregador e necessidades de sustento do empregado. Ainda que o preço, entre tantas regras, seja definido pela Uber, o motorista de fato exerce sua vontade, sem ‘chefe’ direto, presencial e humano procedendo com a verificação de suas atividades. O motorista tem sim autonomia para decidir seus horários e localidades, até com o apoio tecnológico do aplicativo. Se as condições climáticas não são as melhores para dirigir, caso esteja indisposto ou com problemas pessoais que requeiram ausentar-se da prestação dos serviços, o motorista não é penalizado, como o empregado CLT que tem um mísero dia para acompanhar seu filho de até 6 anos em consulta médica. Poderia ser levantado o questionamento que o motorista ao se ausentar não recebe pelas corridas que deixou de executar. Pois bem, a mãe que precisa de mais de um dia para acompanhar seu filho em consulta médica corre os mesmos riscos, incluindo desconto em seu descanso semanal remunerado e de dias no período de férias. A comparação pode causar estranheza, mas reflete os comportamentos e condições das atuais atividades.

[4] Disponível em <https://portal.stf.jus.br/jurisprudenciaRepercussao/verAndamentoProcesso.asp?incidente=6679823&numeroProcesso=1446336&classeProcesso=RE&numeroTema=1291>. Acesso em 13.out.2024.

3 DIFERENTES APLICAÇÕES DA INTELIGÊNCIA ARTIFICIAL NAS RELAÇÕES DE TRABALHO

É mais que evidente o uso da IA e suas ferramentas em todos os aspectos das nossas rotinas. E não é diferente com relação ao trabalho. Desde um simples processo seletivo a uma complexa decisão, a aplicação de meios inteligentes não restritos às competências humanas é até mesmo um meio seguro e isonômico de garantir algum êxito no processo.

Tomando como exemplo o corriqueiro processo seletivo em uma empresa de médio porte, era comum que em determinado momento o departamento responsável pela seleção e contratação recebesse a indicação de algum líder a fim de suprir a vaga e atender uma demanda extraordinária. Revestida de certa ética e exigências de compliance, a prática vem sendo menos usual decorrente também da aplicação de algoritmos junto aos sites de cadastro de *currículo vitae*. Ou seja, a IA deixa menos suscetível a liberalismos ou subjetividades a seleção de um profissional. Essa robotização auxilia, agiliza e isenta as preferências pessoais, mas também combina dados de uma série de plataformas e redes sociais, que nem sempre seriam objeto de um questionamento em entrevista. Isto é, rotinas e postagens em redes sociais podem estar favorecendo ou prejudicando a escolha de um profissional. Outro aspecto é que excelentes profissionais, menos habituais em transformar seus CVs em anúncios atrativos, têm sido negligenciados. A rigidez dos parâmetros pré-fixados pela ferramenta de seleção, em alguns casos, não permite a triagem de um único profissional. Temos o impasse das vagas não preenchidas por falta de capacitação do profissional nos ditames da IA, face a disponibilidade de mão de obra sedenta por uma oportunidade de trabalho.

Já no dia a dia, talvez a IA pudesse ser mais promissora e colaborativa para minimizar os desgastes e o sem-número de reclamações trabalhistas peticionadas diariamente. O Relatório Geral da Justiça do Trabalho 2023[5] aponta que 59,6% das demandas trabalhistas são das atividades de serviços, indústria, comércio e transporte, onde a multa de 40% do FGTS figura em 1º lugar nos assuntos mais recorrentes. A questão é se não existe meios da IA colaborar para que assuntos tão frequentes na Justiça do Trabalho pudessem ser previamente solucionadas, aliviando o judiciário para as questões que de fato exigem o conhecimento insubstituível do juiz.

[5] Relatório Geral da Justiça do Trabalho. Disponível em: <https://tst.jus.br/web/estatistica/jt/relatorio-geral#:~:text=No%20ano%20de%202023%2C%20foram,produtividade%20da%20Justi%C3%A7a%20do%20Trabalho>. Acesso em 08.out.2024.

Nesta seara, corre-se o risco de altivar o temor pela IA substituir o judiciário. Todavia, poderia ser exatamente o oposto. Ou seja, liberar o sufocado judiciário para fazer aquilo que não pode ser objeto de substituição. Popularmente, "não quero que a IA faça arte e escreva enquanto eu lavo a roupa e a louça. Quero que a IA lave a roupa e a louça enquanto eu faço arte e escrevo[6]".

4 RISCOS E OPORTUNIDADES DA IA

Os dados pessoais que, alguns deles, já foram expostos em livros distribuídos gratuitamente nas residências – leia-se lista telefônica – hoje têm tratamento cauteloso, previsto em legislação especial. Empresas têm feito malabarismo para atender a Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD). Isto porque, os dados de seus empregados precisam ser protegidos contra divulgação. São os denominados "dados sensíveis" relacionados a "origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, dados genéticos ou biométricos, quando vinculados a uma pessoa natural[7]". Obviamente, a empresa não deve fazer uso desses dados. Mas uma parcela significativa da população já expõe esses dados inconscientemente nas redes sociais. Se por força da LGPD a empresa não pode tratar dados sensíveis, ela se utiliza dos mesmos para decidir sobre o recrutamento. No mínimo, controverso, não?!

A IA na automatização de atividades repetitivas, como por exemplo no universo dos advogados, traz vantagens significativas em termos de tempo e conteúdo a ser analisado em contratos extensos, simplificando a identificação de cláusulas que merecem maior atenção e correção, por exemplo. Também já é usual na organização de documentos, gestão de prazos, triagens, padrões de decisões, entre tantas aplicações que visam aliviar as rotinas e possibilitar que sejam concentrados esforços em atribuições mais sagazes. Questiona-se se essas facilidades podem trazer riscos ao exercício da advocacia, tais como recursos judiciais elaborados por ChatGPT ou aplicações similares. A própria IA vem dando essa resposta exemplarmente, até aqui. Pois já temos casos de identificação dessas práticas, devidamente notificadas aos órgãos

[6] Frase extraída de Rede Social, sem indicação de autor.
[7] Inteligência artificial: visões interdisciplinares e internacionais. Coordenadora Silmara J. de A. Chinellato. Organizador Eduardo Tomasevicius Filho. São Paulo: Almedina, 2023. p. 145.

competentes, incluindo o Tribunal de Ética e Disciplina (TED) para providências junto aos profissionais.

Cabe destacar que último Nobel de Física (2024) concedeu o prêmio a dois físicos "por descobertas e invenções fundamentais que possibilitam o aprendizado de máquina com redes neurais artificiais[8]".

O ultimato "decifra-me ou te devoro", se é que de fato foi proferido pela Esfinge de Tebas, parece não ser aplicável aos assuntos de inteligência artificial, como alguns gurus de TI defendiam. Experiências diversas têm demonstrado que podemos avançar sem que sejamos devorados ou consumidos pela tecnologia. Entretanto, aqueles que não se adaptarem ou que não buscarem meios de 'cruzarem a esfinge', serão devorados de qualquer forma, seja pela rotina, pela alienação a evolução, pela dependência de subsídios públicos.

Exemplo clássico é o da datilógrafa de outrora que evoluiu para uma secretária proativa capaz de gerenciar boa parte da estrutura administrativa de uma empresa. A máquina de escrever virou peça vintage, sem utilidade prática. A profissional adaptou-se em todos os sentidos profissionais e pessoais, deixando de lado a submissão de outros tempos, hoje facilmente caracterizada como assédio. Ajuste-se ou serás devorado, seria a frase mais apropriada para os dias atuais.

Então, se nos aspectos de competências profissionais e habilidades pessoais observamos progressos, por que o mesmo não acontece com as relações de trabalho? Insistimos no tradicional modelo. Insistimos em manter a litigiosidade na Justiça do Trabalho, com mais de 5 milhões de ações em curso[9]. Insistimos em não reconhecer que a IA pode mudar os nossos contratos de trabalho, sem que isso nos prejudique mais do que seriamos prejudicados pela ausência de trabalho.

A velocidade dos avanços tecnológicos e o emprego da IA em novos segmentos trazem mais oportunidades que riscos. E os riscos – aparentemente – são passíveis de mitigação, conciliação entre partes em caso de litígio e aprimoramento de regras para evolução dos serviços prestados em consonância com as relações de trabalho.

[8] Disponível em <https://www.abc.org.br/2024/10/08/nobel-de-fisica-2024-descobertas-e-invencoes-que-contribuem-para-o-treinamento-de-ia/>. Acesso em 09.out.2024.
[9] Disponível em <https://www.conjur.com.br/2024-out-12/barroso-elogia-dinamica-economica-brasileira-e-critica-litigiosidade-trabalhista/>. Acesso em 13.out.2024.

Cabe destaque a recomendação indicada no relatório do FMI, referenciado anteriormente:

> Zelar para que **os benefícios dessa possível revolução sejam compartilhados de modo mais uniforme**, não apenas dentro dos países, mas também entre regiões e países, pode exigir uma realocação de capital e mão de obra a partir de regiões menos desenvolvidas. Com investimento suficiente, a IA pode ajudar as economias de mercados emergentes e em desenvolvimento a dar um salto em determinados setores, facilitando a relocalização de uma gama mais ampla de tarefas e, assim, reduzindo a desigualdade entre os países. (g.n.)

Ainda de acordo com o mesmo relatório, pessoas com mais acesso à educação têm melhores condições de atuarem em segmentos mais complexos e menos afetados pela IA; enquanto aqueles com menos escolaridade e atuação em empregos de baixa complementaridade são os mais ameaçados pela IA.

CONCLUSÃO

Inteligência artificial é assunto do mais recente livro lançado pelo Ministro Luís Roberto Barroso, que acumula outros tantos títulos relacionados aos direitos humanos, direito constitucional e revolução tecnológica. Na obra "Inteligência Artificial, Plataformas Digitais e Democracia – Direito e tecnologia no mundo atual", o ministro afirma que a IA pode ajudar a "empurrar a história na direção do bem, da justiça e do avanço civilizatório[10]" e defende que o assunto seja brevemente regulamentado.

LGPD, criptomoedas e bets (apostas esportivas) acabaram sendo regularizadas com legislação relativamente atrasada no sentido de que muito já estava acontecendo quando suas respectivas leis foram sancionadas. Parece que o mesmo ocorrerá com a IA. Há um projeto de lei de iniciativa do Senador Rodrigo Pacheco, de maio de 2023. De acordo com a tramitação, divulgada na atividade legislativa do Senador Federal, a audiência pública realizada em setembro de 2024 contou com a participação de especialistas de conselhos internacionais, membros da Confederação Nacional da Indústria e estudiosos de institutos de tecnologia. O art. 17 do PL indica ser de alto risco os sistemas de IA para finalidade de "tomada de decisões sobre promoções ou cessações de relações contratuais de trabalho[11]", entre outros.

[10] BARROSO, Luís R. Inteligência artificial, plataformas digitais e democracia: Direito e tecnologia no mundo atual. 1. ed. – Belo Horizonte: Editora Forum, 2024.
[11] Disponível em <https://www25.senado.leg.br/web/atividade/materias/-/materia/157233>. Acesso em 13.out.2024.

Aguardemos o desfecho deste PL ou de outro que venha a tratar devidamente o assunto 'inteligência artificial'.

Até lá, devemos conviver com o fato de que a IA deve substituir empregos cujas atividades são repetitivas e desprovidas de raciocínios. E devemos, fortemente, atuar para que a educação – básica, fundamental, superior e acessível a todos – possibilite meios de desenvolver habilidades para atuação em processos mais complexos que se utilizem e/ou desenvolvam a IA.

REFERÊNCIAS

ACADEMIA BRASILEIRA DE CIÊNCIAS. **Nobel de Física 2024: descobertas e invenções que contribuem para o treinamento de IA**. Disponível em < https://www.abc.org.br/2024/10/08/nobel-de-fisica-2024-descobertas-e-invencoes-que-contribuem-para-o-treinamento-de-ia/>. Acesso em 09.out.2024.

BARROSO, Luís R. **Inteligência artificial, plataformas digitais e democracia**: Direito e tecnologia no mundo atual. 1. ed. Belo Horizonte: Editora Fórum, 2024.

BRASIL. **Constituição da República Federativa do Brasil**. Brasília, DF: Senado Federal, Coordenação de Edições Técnicas, 2023.

CHINELLATO, Silmara J. de A. **Inteligência artificial**: visões interdisciplinares e internacionais. São Paulo: Almedina, 2023.

CONSULTOR JURÍDICO. **Barroso elogia momento econômico, mas volta a criticar litigiosidade trabalhista**. Disponível em < https://www.conjur.com.br/2024-out-12/barroso-elogia-dinamica-economica-brasileira-e-critica-litigiosidade-trabalhista/>. Acesso em 13.out.2024.

FUNDO MONETÁRIO INTERNACIONAL. **Relatório Anual do FMI 2024**. Disponível em <https://cdn.sanity.io/files/yg4ck731/production/54d1dcaff44e0086c5be9844c78fa54b995c5445.pdf/Portuguese%202024%20IMF%20Annual%20Report.pdf>. Acesso em 20.out.2024.

IBGE. **Instituto Brasileiro de Geografia e Estatística**. Disponível em <https://www.ibge.gov.br/explica/desemprego.php>. Acesso em 20.out.2024.

SENADO FEDERAL. **Projeto de Lei n° 2338, de 2023**. Disponível em <https://www25.senado.leg.br/web/atividade/materias/-/materia/157233>. Acesso em 13.out.2024.

SUPREMO TRIBUNAL FEDERAL. **Tema 1291 - Reconhecimento de vínculo empregatício entre motorista de aplicativo de prestação de serviços de transporte e a**

empresa administradora de plataforma digital. Disponível em < https://portal.stf.jus.br/jurisprudenciaRepercussao/verAndamentoProcesso.asp?incidente=6679823&numeroProcesso=1446336&classeProcesso=RE&numeroTema=1291>. Acesso em 13.out.2024.

TEIXEIRA, José Emídio. **Relações de trabalho nem Freud explica**. 1. ed. Rio de Janeiro: Alta Books, 2024.

TRIBUNAL SUPERIOR DO TRABALHO. **Relatório Geral da Justiça do Trabalho 2023**. Disponível em <https://tst.jus.br/web/estatistica/jt/relatorio-geral#:~:text=No%20ano%20de%202023%2C%20foram,produtividade%20da%20Justi%C3%A7a%20do%20Trabalho>. Acesso em 08.out.2024.

7 Information Society and Law
FMU CENTRO UNIVERSITÁRIO

TRAJETÓRIA EPISTEMOLÓGICA DA RELAÇÃO ENTRE TEORIA GERAL DE SISTEMAS, GESTÃO DE RISCOS E GOVERNO ELETRÔNICO

EPISTEMOLOGICAL TRAJECTORY OF THE RELATIONSHIP BETWEEN GENERAL THEORY OF SYSTEMS, RISK MANAGEMENT AND ELECTRONIC GOVERNMENT

Marcus Vinicius Moreira Zittei[1]

Resumo: Governo eletrônico é a utilização de tecnologia da informação e comunicação nos processos governamentais, tanto para operações internas, quanto transações com a sociedade. Esse processo de implantação provoca mudanças nas organizações e estas mudanças trazem novos riscos. A literatura apresenta que, em processos de mudanças, os riscos são majorados, pois surgem novas relações ainda não conhecidas. Uma base para o entendimento dessas relações é a teoria geral de sistemas, que propicia o estudo integrado dos diversos elementos que interagem em um contexto no qual as empresas são sistemas vivos, dinâmicos e complexos. Este estudo objetiva analisar a trajetória epistemológica da relação entre a teoria geral de sistemas, gestão de riscos e governo eletrônico. O relacionamento ocorre nos estudos em três estudos de Richardson em 1991, 1997 e 2004 influenciados por sistemas indagadores de Churchamn e sistemas dinâmicos de Forrester estudaram governo eletrônico; ocorrendo também no estudo de Hatfield e Hipel em 2002 que analisaram Gestão de Riscos Corporativos na visão sistêmica na perspectiva da TGS; e por fim, Kutsikos e Kontos em 2011 que relacionaram TGS, GRC e EGOV.
Palavras-Chave: Epistemologia; Teoria Geral de Sistemas, Gestão de Riscos, Governo Eletrônico.

Abstract: Eletronic Government is the use of information and communication technology in government processes, both for internal operations, as transactions with the company. This deployment process causes changes in organizations and these changes cause risks. The literature shows that in change processes, the risks are increased because new relationships not known yet arise. To understand these relationships, the general systems theory provides the integrated approach, where companies are considered living, dynamic and complex systems. This study aims to analyze the epistemological trajectory of the relationship between general systems theory, risk management and e-government. The relationship occurs in studies in three Richardson studies in 1991, 1997 and 2004 influenced by Churchamn's inquiring systems and Forrester's Dynamic Systems studied e-government; also occurring in the study by Hatfield and Hipel in 2002 that analyzed Corporate Risk Management in the systemic perspective from the TGS perspective; and finally, Kutsikos and Kontos in 2011 that related TGS, GRC and EGOV.
Keywords: Epistemology; General Systems Theory, Risk Management, Electronic Government.

[1] Doutor em Ciências Contábeis e Administração, Mestre em Ciências Contábeis, Contador, Professor.

INTRODUÇÃO

As organizações estão há muitos anos utilizando a tecnologia para agilizar e otimizar seus negócios – a contabilidade acompanha essa evolução –, com um número cada vez maior de transações, informações, dados, sendo interpretados no tempo ideal para que as decisões também sejam tomadas no tempo certo, e os governos também se utilizam desses avanços.

Desde os anos 1950, os governos em várias partes do mundo organizaram suas atividades internas, procurando mais eficiência e eficácia no trato da coisa pública (BACKUS, 2001), com a preocupação de ter conhecimento do que realmente acontecia, porquanto, o dinheiro não é infinito, e sem uma gestão adequada não se governa (YILDIZ, 2007). A Organização da Nações Unidas (ONU) entendeu que esse processo poderia auxiliar muitas nações, tanto quanto missões humanitárias ou de paz, pois não basta socorrer as pessoas, é preciso também proporcionar uma continuidade e um histórico nas informações de governo, independente dos governantes, uma vez que esses passam, mas o Estado permanece (WORLDBANK, 2011).

Se as organizações empresariais têm a necessidade de gestores e esses de ter governança – participação, transparência e prestação de contas – para o bom funcionamento, o Estado também, além de ter governo, precisa de governança. Com a evolução das tecnologias de informação e comunicação, esse processo passou para governo eletrônico e governança eletrônica. Um processo integrado, no qual estruturas, processos e ideias podem ser criadas ou alteradas provocando, em função do uso das TIC, a evolução da governança (e-governança) e, em paralelo, do governo, já que esse deixa de fazer manualmente os processos e passa a executá-los digitalmente (e-governo).

Todas as mudanças – principalmente aquelas que aumentam as interações e transações –, fazem com que os sistemas fiquem ainda mais complexos. Nessa complexidade, aumentam as incertezas (). Surge o receio das dúvidas prejudicarem as decisões. Porém, a dúvida é necessária à vida, pois ela proporciona análise e reflexão sobre os riscos e, em consequência, pode levar às melhores escolhas.

Desde a década de 1950, com avanço tecnológico e com a utilização da cibernética, a sociedade percebeu que não basta ter apenas garantias para suportar riscos, é basilar possuir ferramentas e condições de gerenciar todo o processo. Assim, com esses avanços, já é possível, antes mesmo de iniciar um novo negócio, por exemplo, prever incertezas. Durante seu

desenvolvimento e existência, podem-se identificar novos riscos, gerenciá-los e, desse modo, tomar decisões de acordo com os interesses e limites da organização e dos investidores.

A ciência ajuda a entender o funcionamento das coisas, apresenta ferramentas teóricas e métodos. A Teoria Geral de Sistemas (TGS) oferece a visão do todo, uma visão holística sobre os fenômenos, interpretando não apenas uma parte isolada, mas todas as interações e possibilidades (ARENA; ARNABOLDI; AZZONE, 2010).

As organizações são sistemas, do tipo social e dinâmico. Formadas por inúmeros subsistemas e com muitas inter-relações e interconexões, são algo vivo e complexo. Sendo formadas por pessoas, a subjetividade das decisões dinamiza o funcionamento do sistema empresa (CHURCHMAN, 1971; MORIN, 2015).

Surgem assim possibilidades de investigação, e este estudo tem por objetivo analisar a trajetória epistemológica da relação entre a Teoria Geral de Sistemas, Gestão de Riscos e Governo Eletrônico. Contribuir por apresentar a continuidade da aplicação teórica proposta por Churchman na administração das organizações e no trato com os entes públicos.

Metodologicamente o trabalho é um estudo epistemológico de três disciplinas especificas (Teoria Geral dos Sistemas, Gestão de Riscos e Governo Eletrônico), analisando as pesquisas teóricas até o momento onde as três se relacionam. Este estudo não se propõe em fazer um resgate histórico das disciplinas, portanto o levantamento de cada temática encerra no ponto onde surge o relacionamento e contribuição com a outra temática.

1 TRAJETÓRIA EPISTEMOLÓGICA

Esta seção expõe o histórico da teoria geral dos sistemas, a partir do seu surgimento e passando pelos principais fatos até o momento em que contribui com as ciências administrativas. Em seguida, trata do desenvolvimento da gestão de riscos corporativo, com as contribuições da TGS e impactos no governo eletrônico. Finalmente, aborda a teorização do governo eletrônico.

1.1 Teoria Geral dos Sistemas

Ludwig von Bertalanffy criou a Teoria Geral dos Sistemas (TGS) em 1937 e a desenvolveu em diversos artigos nas décadas de 1930, 1940 e 1950. Em 1968, apresentou a

consolidação desses estudos em um livro – no Brasil, em 2012, foi lançada a sexta edição desse livro (MORGAN, 1996).

Bertalanffy (2012) buscou, com a TGS, entender a complexidade do todo, contrapondo-a à fragmentação científica. Ele iniciou seus estudos na biologia, não obstante, proporcionou elementos que podem ser utilizados em diversos campos da ciência, como sociologia, psicologia e ciências sociais. Ofereceu, também, características para um sistema aberto, onde acontece a "troca de matéria com o seu ambiente" (BERTALANFFY, 2012, p.186), representando entrada de insumos e saídas de produtos.

Sistema é definido como um conjunto de partes interligadas, que se afetam mutuamente, e são dependentes entre si e, ao mesmo tempo, do todo que formam. Para compreender o sistema é necessário entender o todo e as partes, bem como as inter-relações estabelecidas entre elas (BERTALANFFY, 2012). Desse modo, se só uma parte do sistema for conhecida, é possível estudar apenas essa parte. Talvez seja crível transformá-la num sistema, ou talvez não. Se ela for muito pequena, é mais provável que não possa vir a ser um novo sistema, sequer um subsistema do macrossistema, mas sim, seja somente um elemento de um sistema (WEBER; PÓLO, 2007; BERTALANFFY, 2012).

Tome-se um livro como exemplo de sistema: 'sistema livro'. Ao visualizar o livro inteiro, é possível entender e explicar o 'sistema livro'. No entanto, se for tomada somente uma página, não será possível explicar o 'sistema livro' considerando apenas essa página; porém, pode-se definir essa página como um novo sistema (ou subsistema do macrossistema) e analisar e explicar o 'sistema página'. Agora, se da página, for selecionada apenas uma palavra, será possível analisar essa palavra, mas não será possível compreender nem o 'sistema página', nem o 'sistema livro' por meio dela. Quando a parte é muito pequena, provavelmente ela é um elemento do sistema e não um possível novo sistema ou subsistema dentro do macrossistema (WEBER; PÓLO, 2007; BERTALANFFY, 2012).

O economista Weber e Pólo (2007) buscou, na mesma época que Bertalanffy, relacionar aspectos gerais do mundo empírico com a TGS, apresentando um quadro sistêmico e objetivos da teoria. Ele foi o pesquisador que trouxe a TGS – teoria originalmente das ciências biológicas –, para as ciências aplicadas.

Conforme Boulding (1956, p.9), Boulding não quis estabelecer uma teoria que desse conta de tudo, mas tinha necessidade de um "[...] quadro que contivesse os relacionamentos

gerais do mundo empírico". Sua intenção era encontrar um meio termo entre uma teoria que abarcasse tudo (geral) e teorias que explicassem as partes do todo (especificas). Martinelli et al. (2012), então, estrutura uma hierarquia de sistemas (ou quadro sistêmico), com o pensamento de que existem sistemas e subsistemas participantes de um conjunto maior de sistema. Boulding (1956) apresenta nove níveis nesse 'sistema de sistemas' – interessam para esta pesquisa os quatro primeiros, porque são os que se relacionam com o sistema empresa e com o método aqui aplicado, qual seja o de Boulding (1956). A hierarquia inicia-se com a estrutura – o desenho do todo. O próximo nível abarca a dinâmica simples, os movimentos naturais dentro do conjunto. O terceiro nível é uma parte essencial do sistema, com os mecanismos de controle e o sistema cibernético, no qual as informações são transmitidas e interpretadas. O sistema aberto está presente no quarto nível, onde começa a vida, tanto de um organismo quanto de uma organização, ocorrendo trocas metabólicas: alimentação / processamento / produtos.

Quadro 1 – Quadro sistêmico de Boulding

Níveis	Definição
Estrutura	Estruturas estáticas, relações anatômicas
Mecanismo de relógio	Sistemas dinâmicos simples, movimentos predeterminados. Podem ser modelados como sistemas de equações diferenciais
Termostatos	Mecanismos de controle cibernéticos de transmissão incorporada e interpretação de informações na operação de sistema
Sistemas abertos	Estrutura de manutenção autônoma. Este é o nível em que a vida começa a diferenciar de não-vida: ele pode ser chamado o nível da célula.
Plantas	Sistemas de crescimento, divisão do trabalho, equifinalidade
Animais	Sistemas cientes, mobilidade e teleologia
Humanos	Sistemas de autoconsciente, idioma, simbolismo
Sistemas simbólicos	Sistemas de significado, produtos da consciência humana
Sistemas sociais	Relações de poder, intercâmbio e cooperação

Fonte: Adaptado de Churchman (1971).

Boulding (1956) estudou a TGS com a intenção de demonstrar sua aplicabilidade na área de administração. Por meio de sua pesquisa, ele realizou uma tradução da TGS, originária da biologia, para a gestão. Ou seja, as premissas biológicas foram vertidas para a estrutura organizacional.

Primeiramente, ele concebeu uma estrutura, com a inserção de elementos – para tornar cada parte do sistema compreensível – e identificou cinco aspectos importantes para interpretar o sistema:

a) ambiente – onde o sistema está inserido;

b) recursos – aquilo que vai entrar (inputs) no sistema e o que vai sair, ou, que o sistema vai produzir (outputs);

c) componentes – diz respeito ao processamento, por exemplo, uma máquina que recebe a matéria-prima de um lado e entrega o produto no outro;

d) administração – como se gerencia todo o sistema;

e) objetivo – para que existe o sistema.

Assim, Churchman (1971) expôs as definições de sistema para administração como um agrupamento de partes coordenadas para realizar um conjunto de finalidades. Portanto, sua principal contribuição para a área da administração foi esta: elaborar um método para estudar as organizações. Por meio desse esquema é possível visualizar o sistema total, desde o ambiente até o objetivo, passando pela interação entre todas as atividades.

Churchman (1971) demonstrou quão complexas são as organizações e sua busca por atingir metas estabelecidas. Com a intenção de buscar soluções para problemas de gerência e controle, Van Gigch (1974) apresentou duas metodologias da TGS para compreensão das organizações:

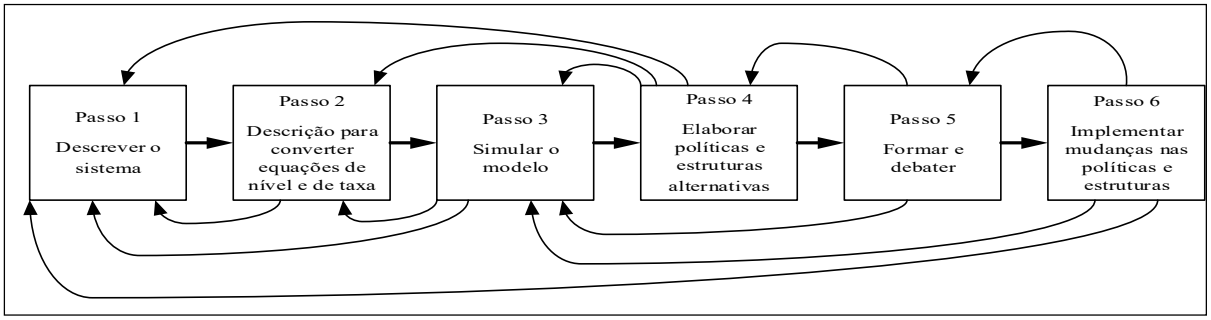
a) hard – representando as ciências exatas, busca quantificação por meio de modelos matemáticos;

b) soft – diz respeito às outras ciências, não se preocupa com a quantificação e sim com o entendimento do sistema como um todo. Nessa metodologia, o sistema – visto como uma parte do ambiente – mantém a identidade mesmo com mudanças. O sistema proporciona estruturas que alteram suas funções no curto prazo, mas sofrem mudanças lentas no longo prazo.

Forrester (1961); Van Gigch (1974) apresenta o conceito de sistema dinâmico: o sistema não é estático, ele se move, trabalha; a cada momento que ocorre um movimento, o sistema volta e recomeça (processo cíclico). Esta concepção de dinamismo dentro do sistema complementa a compreensão de sistema soft de Forrester (1994).

O conceito e a descrição do sistema dinâmico possibilitam a criação de modelos de simulações para interpretar o sistema, isto é, avaliar o comportamento, políticas, escolhas e implementação do sistema em seu ambiente, como apresentado na Figura 1. Van Gigch (1974) apresenta seis passos para demonstrar que um sistema é dinâmico, que para cada etapa é necessário voltar às anteriores para completar o entendimento.

Figura 1 – Passos dos sistemas dinâmicos



Fonte: Forrester (1994)

Forrester (1994) define empresa como um sistema social complexo, "constituída de muitos subsistemas", que pode ser analisado o comportamento de cada um, com interdependência entre os subsistemas. Ou seja, cada um desses subsistemas é correlato ao(s) outro(s) porque dentro do sistema empresa um subsistema interage com outro(s); todavia, dentro de si, cada subsistema tem dinâmica própria e pode ser analisado de forma independente.

Sendo um sistema aberto com diversas interações com os ambientes e constituído de múltiplas funções e relações, a empresa está inserida em um "conjunto de ambientes" (NAKAGAWA, 1987). O ambiente é um dos prismas para se apreender o sistema (NAKAGAWA, 1987), contudo esse ambiente não é algo único, existem inúmeros ambientes – externo e interno (dentro ou fora do sistema), microambiente (relacionamento direto com o sistema) ou macroambiente (relacionamento indireto) –, e esses múltiplos ambientes interagem e influenciam o sistema empresa. Sobre o ambiente não há controle, porém, o ambiente tem ascendência sobre o funcionamento do sistema.

Quando o sistema está em operação, existe movimento interno: esse movimento é gerado pelas trocas – interconexões e inter-relações – entre os elementos do sistema e/ou entre os subsistemas. Nesse ambiente, quando aumenta a quantidade e velocidade dos processos de troca, também aumentam as incertezas e os riscos presentes. Por causa desse crescimento, é fundamental visualizar essas interconexões e inter-relações (CHURCHMAN, 1971).

Um dos primeiros a observar as interconexões e inter-relações foi o pesquisador Weber e Pólo (2007). Na mesma época que Wiener (1948) e Bertalanffy (2012) estavam construindo a Teoria Geral dos Sistemas, Boulding (1956) com outros estavam sintetizando a cibernética. Ele intuía que a TGS e a cibernética continham muito em comum, porém, a cibernética se

diferenciava por ater-se, principalmente, à relação máquina-homem, com o homem exercendo o controle sobre a máquina.

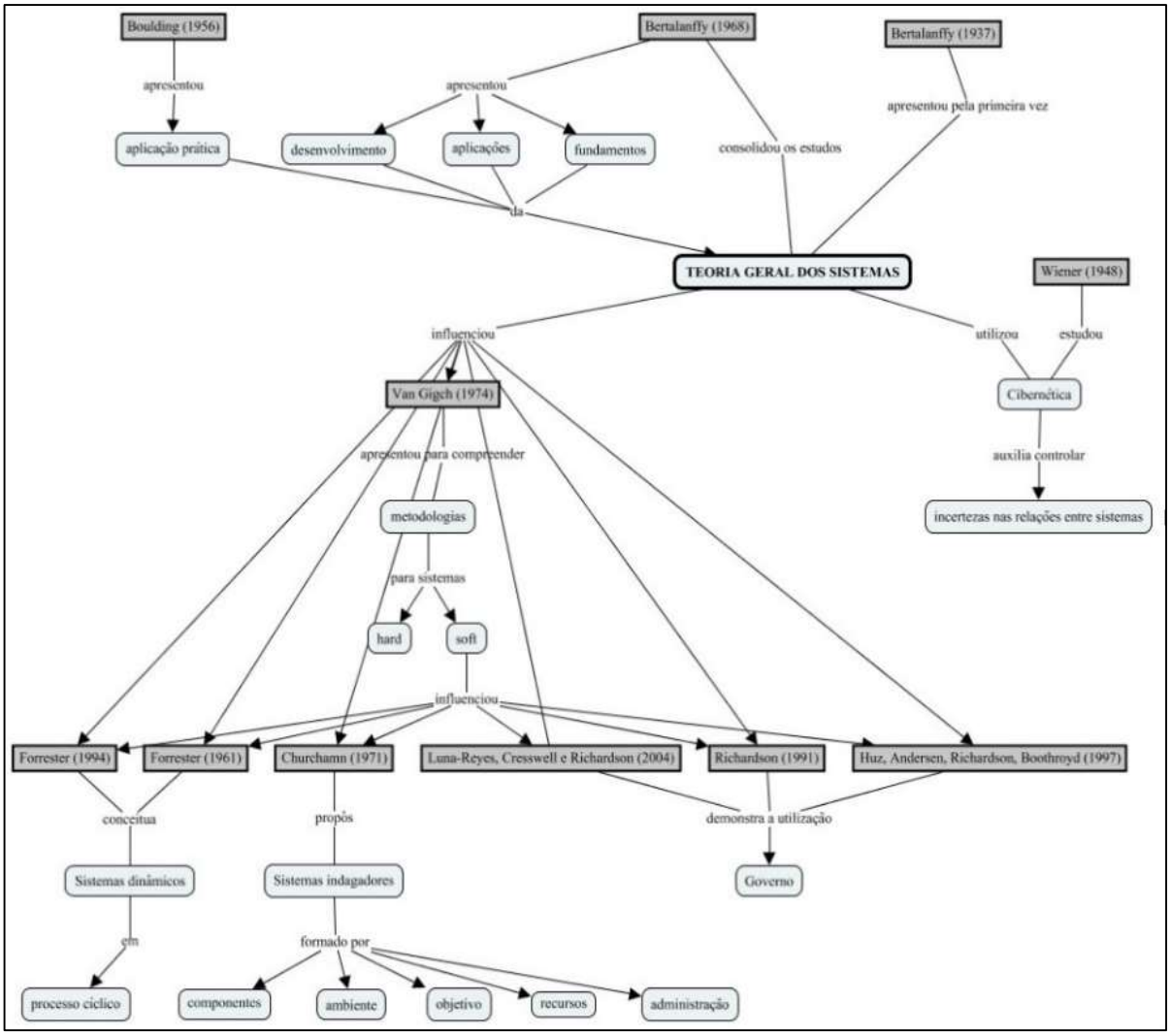
Ao constatar e compreender a existência das interconexões e inter-relações na cibernética, Wiener (1948) entendeu que elas provocavam incertezas e, consequentemente, a necessidade de mecanismos para controlar essas incertezas. A TGS utiliza essas observações da cibernética para evoluir, principalmente na perspectiva da complexidade, pois a cibernética, ao utilizar os princípios matemáticos, consegue abarcar a complexidade.

Wiener (1948) nomearam esses mecanismos de controle das incertezas como sistema de gestão de riscos. A gestão de riscos não precisa se preocupar com um item específico do sistema, ela tem que atentar às relações que os elementos do sistema – componente, recurso, ambiente, administração e objetivo – têm entre si. São nessas interconexões e inter-relações que surgem incertezas, isto é, que existem riscos a serem mitigados e/ou gerenciados.

Pesquisando os sistemas dinâmicos, Hong et al. (2003) apresentou uma integração das Ciências Sociais com a Teoria de Sistemas. Ao desenvolverem pesquisas na gestão pública com esse entendimento, Richardson (1991); Huz et al. (1997) demonstraram a possibilidade de estudar-se questões de governo utilizando-se a TGS.

A Figura 2 apresenta os principais autores e datas desta trajetória. Nela é possível verificar que Luna-Reyes; Cresswell e Richardson (2004) apresentou pela primeira vez a expressão Teoria Geral dos Sistemas, no qual o todo é mais que a soma das partes. Em 1968 o autor consolidou seus estudos apresentando os fundamentos, desenvolvimento e aplicações da TGS, com a ideia de estudar o sistema por meio dos subsistemas, verificando as relações e conexões (BERTALANFFY, 1937). A TGS utilizou a cibernética para o seu desenvolvimento, auxiliando a controlar as incertezas nas diversas relações entre os sistemas (BERTALANFFY, 1968). Wiener (1948) apresenta um quadro sistêmico para aplicação prática da TGS. No estudo das organizações e da gestão, Boulding (1956) propôs cinco aspectos para entendimento dos sistemas: ambiente, recursos, componentes, administração, objetivo. Churchman (1971) apresentou duas metodologias para compreender os sistemas, *hard* e *soft*. Forrester (1961); Van Gigch (1974) conceitua os sistemas como dinâmicos, que se movem, num processo cíclico. Richardson (1991); Forrester (1994); Huz et al. (1997) demonstraram a utilização da TGS para estudar questões relacionadas a governo.

Figura 2 – Trajetória epistemológica da teoria geral dos sistemas



Fonte: Elaborado pelo autor.

1.2 Gestão de riscos corporativos

A gestão de riscos, bem como os debates e estudos sobre o tema, podem ser divididos em três fases: pré-moderna, moderna e pós-moderna. Na primeira fase, são tratados o uso da matemática e estatística na identificação e mensuração dos riscos. Na segunda, inicia o gerenciamento dos riscos – em uma evolução da gestão de seguros para gestão de riscos –, e surgem modelos integrados, nos quais o risco é tratado objetivamente dentro de uma visão sistémica. Na fase atual, o risco é subjetivo, discutido dentro da complexidade da sociedade (SETTEMBRINO, 1994; LUNA-REYES; CRESSWELL; RICHARDSON, 2004; SILVA, 2013).

O momento pré-moderno da gestão de riscos apresentava uma visão objetiva: identificar (saber quem e o que é) e mensurar (quanto é) (MILLER, 2009). Havia um modelo

matemático que reconhecia o risco. Com o risco identificado, entrava em ação o departamento (ou pessoa) responsável, dentro da empresa, por contratar seguros para suportar e/ou não ter prejuízos com esse risco. Não havia a preocupação em entender o risco na busca de soluções ou mitigações, não existia a intenção de gerenciar o risco: sabia-se que havendo o risco "a", deveria ser feito o seguro "b" para proteção. Existiam nas organizações os departamentos de gestão de seguros (MILLER, 2009).

A década de 1950 é a década de transição, quando começam a surgir estudos que relacionam risco com tomada de decisão. O pesquisador francês Miller (2009) critica a escola americana por focar os debates de risco na perspectiva matemática considerando apenas a objetividade nas análises, e apresenta a importância da psicologia comportamental complementar os estudos.

Portanto, na fase moderna da gestão de riscos, fica para trás a visão mecanicista, no qual o risco é tratado como pura matemática. Ao deixar de visualizar o risco apenas como um número ou previsão matemática, o seguro passa a ser um elemento no processo e não mais o ponto central e/ou final (ALLAIS, 1953).

Nessa segunda fase, a subjetividade é incorporada: o risco passa a ser atrelado à tomada de decisão – que é dependente do comportamento humano (GALLAGHER, 1956; MARCH; SHAPIRA, 1987). Surge a preocupação de gerenciar, sair da questão operacional e entender o funcionamento do risco como algo mais elaborado que necessita de coordenação, governança ou gestão (ARROW, 1965). March e Shapira (1987) apontam a preocupação com avaliação e gestão dos riscos. Anteriormente, se houvesse um desastre ambiental, por exemplo, o seguro era pago e fim da questão. A partir dessa fase, passa-se a buscar evitar que o desastre ocorra (WILSON; CROUCH, 2001).

Por fim, o risco será visto como um sistema e abandona-se a postura de somente mitigá-lo por meio de seguros (GALLAGHER, 1956). Através do entendimento de que a organização é um sistema e o risco é um subsistema dentro do sistema, Hatfield e Hipel (2002) destacaram a importância de conhecer este sistema, para que se possa assumir os riscos, com a perspectiva de melhorar segurança na tomada de decisões.

Incorporadas à visão sistêmica dos riscos e a possibilidade de gerenciá-los, surgem os modelos para poder refletir e considerar o risco em todo o seu processo. Esses modelos integrados proporcionaram que se alcançasse gerenciar o risco como um todo e responder: De

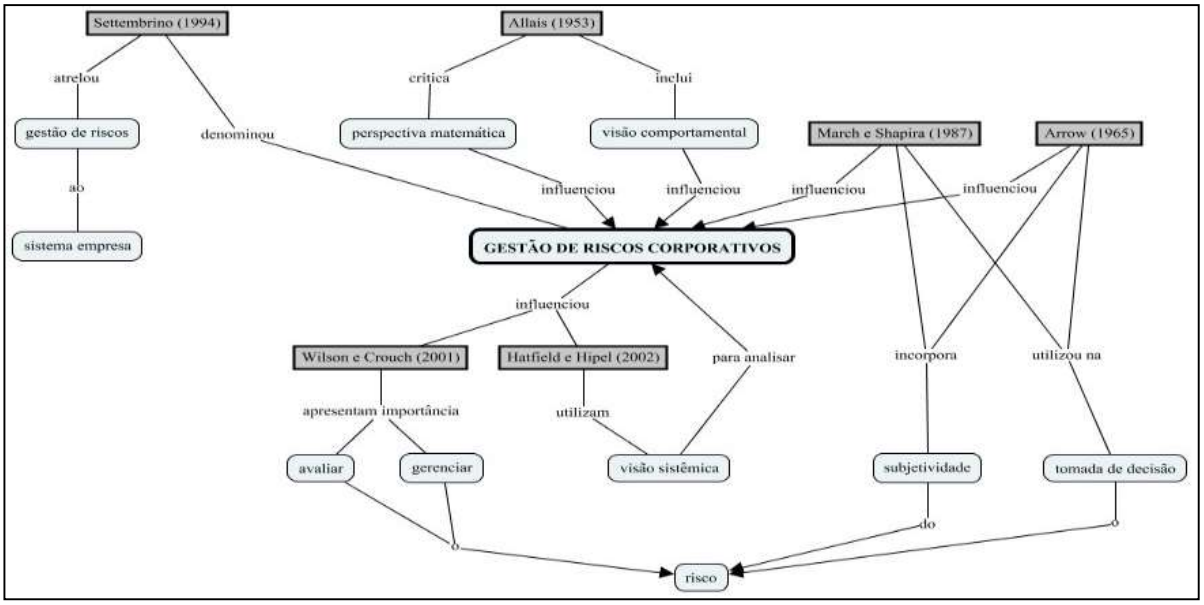
onde ele surgiu? Está atrelado a quais ambientes? Quais seus mecanismos de funcionamento? Assim, passando a interagir com todo o sistema empresa – resultando no que March e Shapira (1987) chamou de gestão de riscos corporativos –, tornou-se possível imaginar o que poderia vir a acontecer, quais os mecanismos de controle, como gerenciar para que não ocorresse o risco.

Na fase pós-moderna existe uma série de mecanismos objetivos – protocolos, regras, controles, indicadores etc. –, para apreender, gerenciar e assumir todos os riscos. Todavia, o sistema empresa é composto por pessoas e por operações que envolvem pessoas e suas escolhas, do que é possível concluir que o comportamento humano influencia fortemente nas decisões de gerenciamento dos riscos, isto é, o sistema empresa está imerso e envolto em complexidade e subjetividade e, por ser complexo, aumentam as interconexões e inter-relações (SETTEMBRINO, 1994).

Com o auxílio da ciência comportamental (psicologia e afins), os estudos sobre gestão de riscos corporativos vão procurar compreender esse lado subjetivo da questão: a decisão humana é influenciada pelos desejos e conhecimentos que as pessoas acumulam. Miller (2009) analisam o risco e a gestão de risco na visão sistêmica, discutindo que a TGS pode contribuir com ferramentas de análise para identificar, avaliar e gerenciar os riscos, tanto em situações simples quanto complexas.

A Figura 3 apresenta os principais autores e datas desta trajetória. Hatfield e Hipel (2002) critica a perspectiva matemática e inclui a visão comportamental. Para Allais (1953); Arrow (1965) a subjetividade do risco é incorporada aos estudos, e o risco utilizado na tomada de decisão. March e Shapira (1987) atrelou a gestão de riscos ao sistema empresa, e denominou a gestão de riscos corporativos. Settembrino (1994) apresentam a importância de avaliar e gerenciar os riscos. Wilson e Crouch (2001) utilizam a visão sistêmica para analisar a gestão de riscos.

Figura 3 – Trajetória epistemológica da gestão de riscos corporativos



Fonte: Elaborado pelo autor.

1.3 Governo eletrônico

Para Hatfield e Hipel (2002, p. 2), governo eletrônico (e-governo, E-GOV) é:

> uma forma de comércio eletrônico na governança e refere-se aos processos e estruturas necessárias para oferecerem serviços electrónicos ao público (cidadãos e empresas), colaborar com parceiros de negócios e para a realização de transações eletrônicas dentro de uma entidade organizacional.

As primeiras experiências de e-governo ocorreram no início da década de 1990. A ONU, preocupada com a conjuntura da África – guerras, constantes mudanças de governos e, consequentemente, ausência de continuidade nos serviços prestados pelo governo –, procurou incentivar a implementação de práticas de administração pública que utilizassem a Tecnologia da Informação e Comunicação(TIC), para que fosse criado um histórico e as informações tivessem perenidade (BACKUS, 2001).

Com os avanços da TIC, vários países começaram a empregar a cibernética e suas ferramentas no intuito de maximizar o uso das informações coletadas. Principiou-se então, com o auxílio da ONU na divulgação, uma interação entre os países. Nos anos 2000, os projetos de governo eletrônico entraram em operação completa: a conexão dessas tendências permitiu aos governos obter maior intercâmbio entre os órgãos governamentais e abriu a possibilidade de interagir com outros segmentos: sociedade, empresas, outros governos (BACKUS, 2001). Esse

autor afirma que com o aprendizado e com os novos conhecimentos será cada vez maior a integração e mudanças nas organizações, tanto públicas quanto privadas.

Quando surge algo novo, a tendência é que as pesquisas sejam sobre seu uso. Nesse caso, até então, os estudos sobre governo eletrônico estavam focados na tecnologia; a intenção era entender o funcionamento de uma ferramenta tecnológica (BACKUS, 2001; YILDIZ, 2007). Em 2005, consolidando os estudos em E-GOV, Meneklis e Douligeris (2010) apresentam um quadro das principais disciplinas envolvidas e os fatores de sucesso das aplicações.

Começam os estudos com menos foco na tecnologia da informação e mais na questão organizacional, com o objetivo de apreender como e-governo impactava na sociedade e nas organizações. Ao procurar compreender e conceituar governo eletrônico, Gil-García e Pardo (2005) demonstram que são várias disciplinas (gestão pública, TIC, direito etc.) que interagem e auxiliam o processo (que é sistêmico) e os fatores críticos de sucesso. No Quadro 2, Gil-García e Pardo (2005) apresenta os fatores críticos de sucesso do EGOV, desde a visão micro até a visão macro do governo eletrônico. No primeiro momento, como as informações e dados são utilizados, para garantir qualidade e a conformidade; em seguida apontam a utilização da tecnologia da informação, como ferramenta de operacionalização do governo eletrônico; incluem os aspectos organizacionais e de gerenciamento, buscando uma estrutura capaz de operacionalizar as demandas de governo eletrônico; consideram a regulamentação dos processos, tanto leis quanto normas internas também como fatores relevantes; e, por fim, avaliam o fator institucional e ambiental, no qual apresentam as relações com os usuários internos e externos, governos e parceiros, com a preocupação da confiança, privacidade e autonomia.

Quadro 2 – Categorias, desafios e fatores críticos de sucesso do EGOV

Categorias	Desafios	Fatores de sucesso
Informações e dados	Qualidade das informações e dados	Retornos contínuos para usuários parceiros
		Garantia de qualidade e conformidade
		Treinamento
Tecnologia da informação	Necessidade de informações dinâmica	Fácil de usar
	Usabilidade	
	Problemas de segurança	
	Incompatibilidade tecnológica	Utilidade
	Complexidade tecnológica	
	Habilidade técnica e experiência	Demonstrações e protótipos
	Inovação tecnológica	
Organizacio-nal e gerencial	Tamanho do projeto	Habilidades e conhecimenots da equipe do projeto

	Atitudes e comportamentos gerenciais	Lider de TIC bem qualificado e respeitado (competências técnicas e sociais)
	Diversidade de usuários ou organizacional	Objetivos claros e realistas
		Identificação das partes interessadas
	Falta de alinhamento dos objetivos da organização e do projeto	Envolvimento do usuário final
		Planejamento
	Metas múltiplas ou conflitantes	Marcos claros e resultados mensuráveis
		Boa comunicação
	Resistência à mudança	Prévia de melhoria de processos de negócios
		Formação adequada
	Áreas e conflitos	Financiamento adequado e inovador
		Revisão em curso ou melhores práticas
Legal e regulatório	Leis e regulamentos restritivos	Políticas e normas de tecnologia da informação
	Orçamentos anuais	
	Relações intergovernamentais	
Institucional e ambiental	Preocupações com a privacidade	Envolvimento do usuário final
	Autonomia das agências	Liderança executiva ou patrocínio
	Política e as pressões políticas	Terceirização estratégica e parcerias público-privadas

Fonte: Adaptado de Gil-García e Pardo (2005).

Os estudos passam a contemplar questões organizacionais, legais, regulatórias, institucionais e ambientais. Gil-García e Pardo (2005) enfatizam que E-GOV não é apenas um avanço tecnológico, outrossim, significa aumentar a participação do usuário no ambiente governamental. Portanto, governo eletrônico, por mais que traga a palavra eletrônico em sua nomenclatura, não é tão-somente um avanço tecnológico que aconteceu na administração pública: trata-se também de proporcionar a participação de mais e diferentes usuários neste ambiente governamental.

Diante desse histórico, pode-se inferir que as pesquisas em E-GOV estavam centradas na visão positivista: o intuito era apresentar as práticas adotadas. Ou estudava-se governo eletrônico como uma ferramenta tecnológica para prestação de serviços, ou avaliava-se seu impacto nas organizações e na sociedade, e poucos são os trabalhos que teorizam sobre E-GOV (IRANI; LOVE; JONES, 2008; LUCIANO; MACADAR; LOPES, 2015).

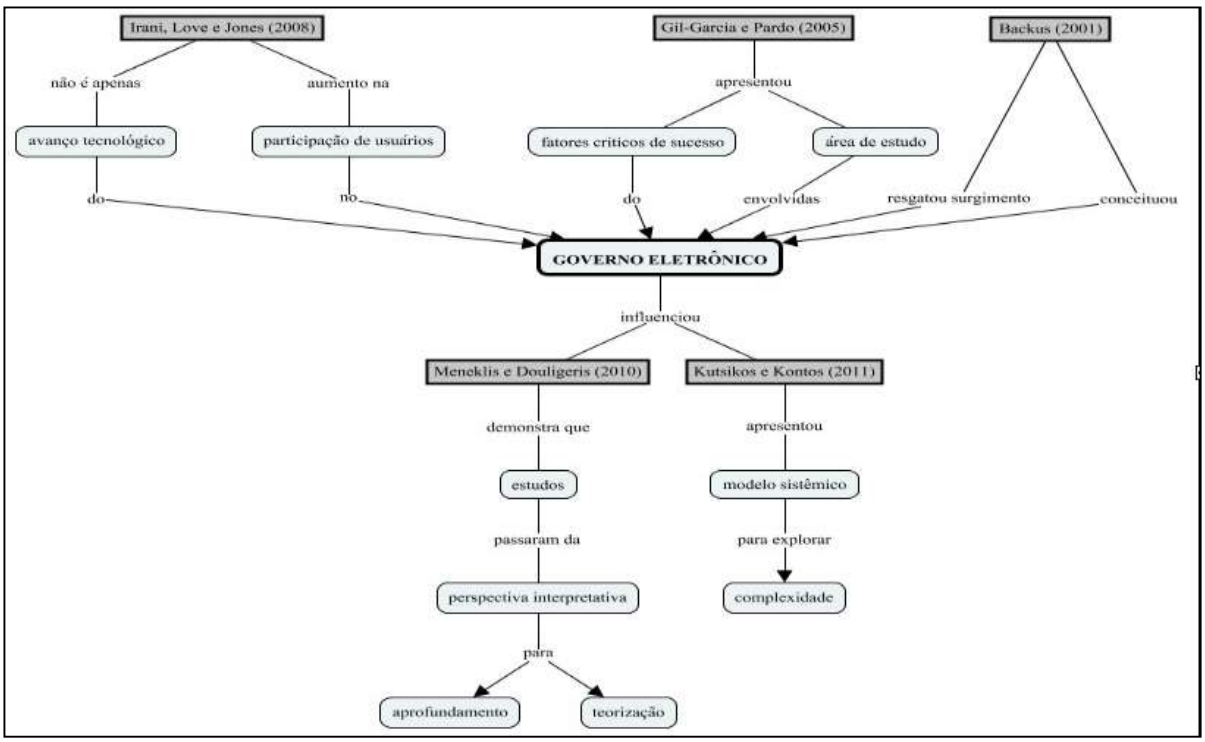
Bannister e Connolly (2015) demonstram que posteriormente houve uma mudança para a perspectiva interpretativa, procurando um aprofundamento dos estudos. Conforme Meneklis e Douligeris (2010), as pesquisas em sistemas de informações (SI) passaram pelas mesmas fases e, com seu avanço, sobreveio esta visão diferente (interpretativa). E-GOV não é uma ferramenta de SI, mas ele se vale das experiências e ferramentas de SI para o seu funcionamento e desenvolvimento (MENEKLIS; DOULIGERIS, 2010).

No Brasil, os estudos (MENEKLIS; DOULIGERIS, 2010; GERON et al., 2011; LAIA et al., 2011; CORDEIRO; KLANN, 2014) se concentram em avaliar o funcionamento do E-GOV. Joia (2009) apresentaram um resgate histórico no Brasil do governo eletrônico e Diniz et al. (2009) avaliaram E-GOV como área de pesquisa, e concluíram em consonância com as pesquisas internacionais (LUCIANO; MACADAR; LOPES, 2015), que é sub-teorizada.

Bannister e Connolly (2015) exploram a complexidade do ambiente de e-governo, com foco na gestão das informações relacionadas. Apresentam um modelo sistêmico (VSM – Modelo de Sistema Viável) como base para modelar um ecossistema de organizações, com a finalidade de gerenciar a complexidade desse ambiente.

A Figura 4 apresenta os principais autores e datas desta trajetória: Kutsikos e Kontos (2011) foi o primeiro autor a conceituar EGOV e resgatar o surgimento do governo eletrônico. Backus (2001) apresentam as principais disciplinas (áreas de estudo) envolvidas e os fatores críticos de sucesso. Gil-García e Pardo (2005) enfocam que não é apenas um avanço tecnológico, mas também um aumento na participação dos usuários no governo. Irani; Love e Jones (2008) demonstram que os estudos passaram da perspectiva interpretativa para um aprofundamento e teorização dessa área de estudo. Meneklis e Douligeris (2010) apresentam um modelo sistêmico para explorar a complexidade do governo eletrônico.

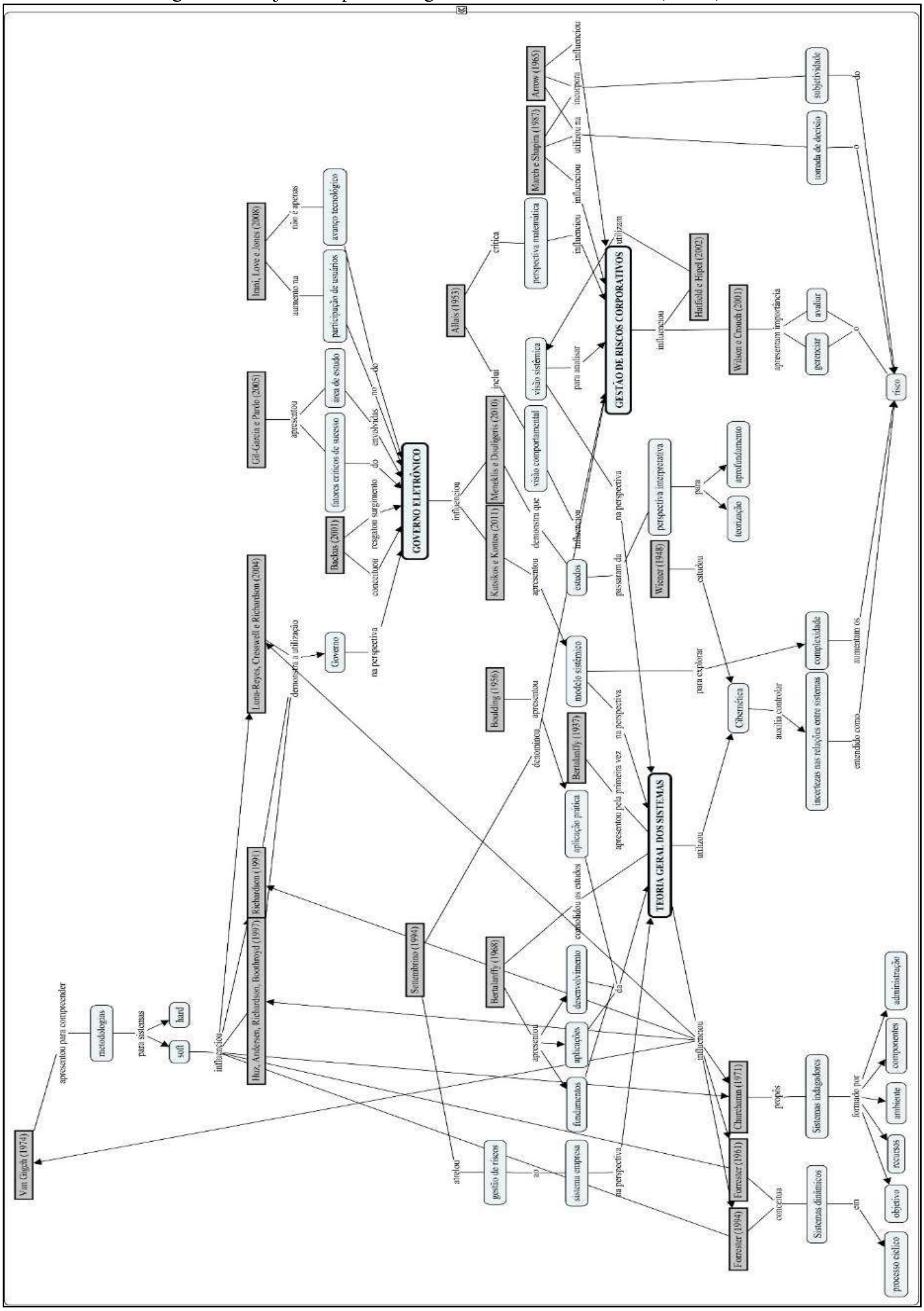
Figura 4 – Trajetória epistemológica do governo eletrônico



Fonte: Elaborada pelo autor.

Do ponto de vista da trajetória epistemológica, o relacionamento da teoria geral de sistemas, gestão de riscos corporativos e governo eletrônico, ocorre nos estudos de Richardson (1991); Huz et al. (1997); Kutsikos e Kontos (2011), com a utilização da TGS para estudar governo, com Luna-Reyes; Cresswell e Richardson (2004) com a utilização da TGS para estudar riscos, e Hatfield e Hipel (2002) utilizando a TGS para estudar governo eletrônico em um ambiente complexo e com muitas inter-relações e interconexões que aumentam as incertezas, como apresentado na Figura 5.

Figura 5 – Trajetória epistemológica do relacionamento TGS, GRC, EGOV



Fonte: Elaborado pelo autor.

CONCLUSÃO

Quando um novo sistema surge, a TGS pode contribuir para entender sua concepção e sua utilização. A literatura relata que Governo Eletrônico ainda é um campo sub-teorizado e fragmentado. A TGS contribui para explorar em partes e componentes do todo de um sistema, e o governo eletrônico – um campo ainda sub-teorizado e fragmentado –, apresenta um campo fértil para o estudo aplicado de diferentes teorias. Esta pesquisa contribuiu para o preenchimento dessa lacuna produzindo um mapeamento sistêmico e apresentando relação entre a TGS, Gestão de Riscos e Governo Eletrônico.

Governo Eletrônico e Gestão de Riscos estão inseridos num contexto complexo, que apresenta muitas inter-relações e interações na perspectiva das organizações (públicas e privadas), sendo assim necessário o estudo do todo e de partes. A Teoria Geral de Sistemas apresenta as metodologias e perspectivas teóricas úteis para estes aprofundamentos, principalmente na proposta dos sistemas indagadores de Churchman.

Conclui-se então que epistemologicamente a relação entre a Teoria Geral de Sistemas, Gestão de Riscos e Governo Eletrônico ocorre quando:

- Richardson em seu estudo de 1991 e com outros pesquisadores (em 1997 com Huz, Andersen e Boothroyd; e 2004 com Luna-reyes, Cresswell) foram influenciados por sistemas indagadores de Churchamn e sistemas dinâmicos de Forrester para demonstrar a utilização da TGS no Governo Eletrônico;
- Hatfield e Hipel em 2002 utilizaram a visão sistêmica na perspectiva da TGS para analisar a Gestão de Riscos Corporativos;
- Kutsikos e Kontos em 2011 fizeram a relação das três disciplinas (TGS, GRC, EGOV). Apresentaram governo eletrônico em um modelo sistêmico na perspectiva da TGS, em um ambiento complexo que aumentam os riscos por ter muitas inter-relações e interconexões (influenciado com as propostas de Churchamn e de Forrester)

Como sugestão de pesquisas futuras o estudo epistemológico em uma visão sistêmica do Governo Eletrônico, pois sendo ainda um campo sub-teorizado, outros estudos poderão apresentar lacunas e a evolução do campo de estudo.

REFERÊNCIAS

ALLAIS, M. Le Comportement de l'Homme Rationnel devant le Risque: Critique des Postulats et Axiomes de l'Ecole Americaine. **Econometrica,** v. 21, n. 4, p. 503-546, 1953. ISSN 00129682. Disponível em: < http://www.jstor.org/stable/1907921 >. Acesso em: 05 set. 2015.

ARENA, M.; ARNABOLDI, M.; AZZONE, G. The organizational dynamics of Enterprise Risk Management. **Accounting, Organizations and Society,** v. 35, n. 7, p. 659-675, // 2010. ISSN 03613682 (ISSN). Disponível em: < http://www.scopus.com/inward/record.url?eid=2-s2.0-78049383775&partnerID=40&md5=6f05796e8ddc167b0c39f0337faa480d >. Acesso em: 05 set. 2015.

ARROW, K. J. **Aspects of the theory of risk-bearing**. Helsinki: Yrjö Jahnssonin Säätiö, 1965.

BACKUS, M. E-governance in Developing Countries: Introduction and examples. **IICD Research Brief,** v. Research Report, n. 3, p. 1-51, 2001. Disponível em: < http://www.iicd.org/about/publications/egovernance-and-developing-countries-introduction-and-examples/report3.pdf >. Acesso em: 05 set. 2015.

BANNISTER, F.; CONNOLLY, R. The great theory hunt: Does e-government really have a problem? **Government Information Quarterly,** v. 32, n. 1, p. 1-11, 1// 2015. ISSN 0740-624X. Disponível em: < http://www.sciencedirect.com/science/article/pii/S0740624X14001634 >. Acesso em: 05 set. 2015.

BERTALANFFY, L. V. **Das Gefüge des Lebens**. Leipzig und Berlin: Verlag und Druck von B. G. Teubner, 1937. iv, [2], 197 p. Disponível em: < http://hdl.handle.net/2027/uc1.b3349065 >. Acesso em: 15 jan. 2016.

BERTALANFFY, L. V. **General system theory : foundations, development, applications**. New York: Braziller, 1968. ISBN 0807604526
0807604534. Acesso em: 15 jan. 2016.

BERTALANFFY, L. V. **Teoria geral dos sistemas: fundamentos, desenvolvimento e aplicações**. 6. ed. Petrópoli, RJ: Vozes, 2012. 360 ISBN 9788532636904.

BOULDING, K. E. General systems theory-the skeleton of science. **Management science,** v. 2, n. 3, p. 197-208, 1956. ISSN 0025-1909. Disponível em: < http://pubsonline.informs.org/doi/abs/10.1287/mnsc.2.3.197 >. Acesso em: 05 set. 2015.

CHURCHMAN, C. W. **The design of inquiring systems: Basic concepts of systems and organization**. Basic books New York, 1971. ISBN 0465016081.

CORDEIRO, A.; KLANN, R. C. Institucionalização de hábitos e rotinas com a implantação do Sistema Público de Escrituração Digital (SPED): um estudo em organizações de serviços

contábeis. **Revista Gestão Organizacional,** v. 7, n. 1, p. 79-93, 2014 2014. ISSN 1983-6635. Disponível em: < http://www.spell.org.br/documentos/ver/34847/institucionalizacao-de-habitos-e-rotinas-com-a-implantacao-do-sistema-publico-de-escrituracao-digital--sped---um-estudo-em-organizacoes-de-servicos-contabeis >. Acesso em: 15 jan. 2016.

DINIZ, E. H.; BARBOSA, A. F.; JUNQUEIRA, A. R. B.; PRADO, O. O governo eletrônico no Brasil: perspectiva histórica a partir de um modelo estruturado de análise. **Revista de Administração Pública,** v. 43, n. 1, p. 23-48, Fev. 2009. ISSN 0034-7612. Disponível em: < http://www.scielo.br/pdf/rap/v43n1/a03v43n1.pdf >. Acesso em: 05 Set. 2015.

FORRESTER, J. W. **Industrial dynamics**. MIT press Cambridge, MA, 1961.

_____. System dynamics, systems thinking, and soft OR. **System Dynamics Review,** v. 10, n. 2-3, p. 245-256, 1994. ISSN 1099-1727. Disponível em: < http://dx.doi.org/10.1002/sdr.4260100211 >. Acesso em: 05 set. 2015.

GALLAGHER, R. B. Risk Management - New Phase of Cost Control. **Harvard Business Review,** v. 34, n. 5, p. 75-86, 1956. ISSN 0017-8012. Disponível em: < <Go to ISI>://WOS:A1956CBJ3700006 >. Acesso em: 15 jan. 2016.

GERON, C. M. S.; FINATELLI, J. R.; FARIA, A. C. D.; ROMEIRO, M. D. C. SPED – Sistema Público de Escrituração Digital: Percepção dos contribuintes em relação os impactos de sua adoção. **Revista de Educação e Pesquisa em Contabilidade (REPeC),** v. 5, n. 2, p. 44-67, Mai/Ago. 2011. ISSN 1981-8610. Disponível em: < http://www.repec.org.br/index.php/repec/article/download/343/128 >. Acesso em: 05 set. 2015.

GIL-GARCÍA, J. R.; PARDO, T. A. E-government success factors: Mapping practical tools to theoretical foundations. **Government Information Quarterly,** v. 22, n. 2, p. 187-216, 2005. ISSN 0740624X (ISSN). Disponível em: < http://ac.els-cdn.com/S0740624X05000158/1-s2.0-S0740624X05000158-main.pdf?_tid=6862f4c0-90fa-11e3-ab59-00000aacb362&acdnat=1391889271_1a0772be9e2bb4a6918ecb5291eec204 >. Acesso em: 05 set. 2015.

HATFIELD, A. J.; HIPEL, K. W. Risk and systems theory. **Risk Analysis,** v. 22, n. 6, p. 1043-1057, Dec 2002. ISSN 0272-4332. Disponível em: < http://onlinelibrary.wiley.com/store/10.1111/1539-6924.00272/asset/1539-6924.00272.pdf?v=1&t=hh9jujj3&s=5558323f3531758472fe9a402677d567cc8c303d >. Acesso em: 05 set. 2015.

HONG, K. S.; CHI, Y. P.; CHAO, L. R.; TANG, J. H. An integrated system theory of information security management. **Information Management and Computer Security,** v. 11, n. 5, p. 243-248, // 2003. ISSN 09685227 (ISSN). Disponível em: < http://www.scopus.com/inward/record.url?eid=2-s2.0-0345327795&partnerID=40&md5=a3048beebf49d8dc7a91ee03ae907b21 >. Acesso em: 05 set. 2015.

HUZ, S.; ANDERSEN, D. F.; RICHARDSON, G. P.; BOOTHROYD, R. A framework for evaluating systems thinking interventions: An experimental approach to mental health system change. **System Dynamics Review,** v. 13, n. 2, p. 149-169, // 1997. ISSN 08837066 (ISSN). Disponível em: < http://www.scopus.com/inward/record.url?eid=2-s2.0-0344980346&partnerID=40&md5=61b032656c56903d5611b0ea8edb9aca >. Acesso em: 05 set. 2015.

IRANI, Z.; LOVE, P. E. D.; JONES, S. Learning lessons from evaluating eGovernment: Reflective case experiences that support transformational government. **Journal of Strategic Information Systems,** v. 17, n. 2, p. 155-164, // 2008. ISSN 09638687 (ISSN). Disponível em: < http://www.scopus.com/inward/record.url?eid=2-s2.0-44149128688&partnerID=40&md5=fed1cf7cfda4c81136f89da8929ea152 >. Acesso em: 05 set. 2015.

JOIA, L. A. Governo eletrônico e capital intelectual nas organizações públicas. **Revista de Administração Pública,** v. 43, n. 6, p. 1379-1405, Dez. 2009. ISSN 0034-7612. Disponível em: < http://www.scielo.br/pdf/rap/v43n6/08.pdf >. Acesso em: 05 set. 2015.

KUTSIKOS, K.; KONTOS, G. A systems-based complexity management framework for collaborative e-government services. **International Journal of Applied Systemic Studies,** v. 4, n. 1-2, p. 1-16, // 2011. ISSN 17510589 (ISSN). Disponível em: < http://www.scopus.com/inward/record.url?eid=2-s2.0-80052348683&partnerID=40&md5=72c4e68acb71fa1436bbf15a5249c86d >. Acesso em: 05 set. 2015.

LAIA, M. M. D.; CUNHA, M. A. V. C. D.; NOGUEIRA, A. R. R.; MAZZON, J. A. Políticas de Governo Eletrônico no Brasil: Contexto, Gestão de Tic e Resultados. **2011,** v. 51, n. 1, p. 043-057, jan./fev. 2011. ISSN 0034-7590. Disponível em: < http://bibliotecadigital.fgv.br/ojs/index.php/rae/article/view/31005/29819 >. Acesso em: 05 set. 2015.

LUCIANO, E. M.; MACADAR, M. A.; LOPES, K. M. G. **Governo Eletrônico no Brasil: uma área de pesquisa sub-teorizada?** XVIII SEMEAD. São Paulo: FEA-USP. Anais 2015.

LUNA-REYES, L. F.; CRESSWELL, A. M.; RICHARDSON, G. P. Knowledge and the development of interpersonal trust: A dynamic model. In: SPRAGUE JR, R. H., 2004, Big Island, HI. p.1369-1380.

MARCH, J. G.; SHAPIRA, Z. MANAGERIAL PERSPECTIVES ON RISK AND RISK TAKING. **Management Science,** v. 33, n. 1, p. 1404-1418, 1987. ISSN 00251909. Disponível em: < http://www.scopus.com/inward/record.url?eid=2-s2.0-0023456474&partnerID=40&md5=dbf0e743417c39a85f30bb991a73aeac >. Acesso em: 05 set. 2015.

MARTINELLI, D. P.; VENTURA, C. A. A.; LIBONI, L. B.; MARTINS, T. M. **Teoria geral dos sistemas**. São Paulo: Saraiva, 2012. ISBN 9788502180383.

MENEKLIS, V.; DOULIGERIS, C. Studying the Interaction of the Epistemology in e-Government, Organization Studies and Information Systems. In: SIDERIDIS, A. e PATRIKAKIS, C. (Ed.). **Next Generation Society. Technological and Legal Issues**: Springer Berlin Heidelberg, v.26, 2010. cap. 7, p.79-86. (Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering). ISBN 978-3-642-11629-2.

MILLER, K. D. Organizational Risk after Modernism. **Organization Studies,** v. 30, n. 2-3, p. 157-180, Feb 2009. ISSN 0170-8406. Disponível em: < http://oss.sagepub.com/content/30/2-3/157.full.pdf >. Acesso em: 05 set. 2015.

MORGAN, G. **Imagens da organização**. Atlas, 1996. ISBN 9788522424658. Disponível em: < http://books.google.com.br/books?id=xsZQAgAACAAJ >. Acesso em: 05 set. 2015.

MORIN, E. **Introdução ao pensamento complexo**. 5 ed. Porto Alegre: Sulina, 2015. 120 p.

NAKAGAWA, M. **Estudo de alguns aspectos de controladoria que contribuem para a eficácia gerencial**. 1987. 165 p. Doutorado em Controladoria e Contabildiade (Tese). Departamento de Contabilidade e Atuária, Faculdade de Economia, Administração e Contabilidade. Universidade de São Paulo

RICHARDSON, G. P. **Feedback Thought in Social Science and Systems Theory**. Philadelphia: University of Pennsylvania Press, 1991.

SETTEMBRINO, F. Risk management in enterprise: a systemic approach. **Risk Management,** v. 41, n. 8, p. 34+, 1994/08 1994. ISSN 00355593. Disponível em: < http://go.galegroup.com.ez71.periodicos.capes.gov.br/ps/i.do?id=GALE%7CA15724496&v=2.1&u=capes&it=r&p=AONE&sw=w&asid=3e67186656596f711589692d7fbad11e >. Acesso em: 16 set. 2015.

SILVA, M. Z. D. **Gerenciamento de riscos corporativos sob o enfoque da teoria contingencial :estudo de caso em uma organização hospitalar**. 2013. 285 Tese (Doutorado). Programa de Pós-Graduação em Ciências Contábeis e Administração, Universidade Regional de Blumenau, Blumenau.

VAN GIGCH, J. P. **Applied general systems theory**. Harper & Row New York, 1974. ISBN 0060467754.

WEBER, W.; PÓLO, E. F. A Imprecisão na Administração Estratégica: uma abordagem baseada no pensamento complexo. **2007,** v. 9, n. 24, p. 16, 2007-08-29 2007. ISSN 1983-0807. Disponível em: < http://rbgn.fecap.br/RBGN/article/view/80 >. Acesso em: 05 set. 2015.

WIENER, N. Cybernetics. **Scientific American,** v. 179, n. 5, p. 14-19, 1948. ISSN 00368733. Disponível em: < http://www.scopus.com/inward/record.url?eid=2-s2.0-33749595028&partnerID=40&md5=74528f49518fb35e771772da4c1fa672 >. Acesso em: 05 set. 2015.

WILSON, R.; CROUCH, E. A. C. **Risk-benefit analysis**. 2 ed. Cambridge: Center for Risk Analysis Harvard University, 2001.

WORLDBANK. Definition of E-Government. 2011. Disponível em: < http://www.worldbank.org/egov/ >. Acesso em: 05 Set. 2015.

YILDIZ, M. E-government research: Reviewing the literature, limitations, and ways forward. **Government Information Quarterly,** v. 24, n. 3, p. 646-665, Jul 2007. ISSN 0740-624X. Disponível em: < http://ac.els-cdn.com/S0740624X07000056/1-s2.0-S0740624X07000056-main.pdf?_tid=74587ec0-256c-11e3-a2b7-00000aacb35e&acdnat=1380063529_98f91144b184e41c644de85bd8ea55e4 >. Acesso em: 05 set. 2015.

7 Information Society and Law
FMU CENTRO UNIVERSITÁRIO

A INTELIGÊNCIA ARTIFICIAL, O DESEMPREGO E A FALTA DE REGULAMENTAÇÃO NO BRASIL

ARTIFICIAL INTELLIGENCE, UNEMPLOYMENT AND THE LACK OF REGULATION IN BRAZIL

Luís Filipe Fernandes Ferreira[1]

Resumo: A inteligência artificial (IA) está cada vez mais presente no dia a dia de todos, impactando a forma como se obtém notícias, como uma pessoa pesquisa e compara preços de produtos, como nos deslocamos ao trabalho, como definimos a contratação de um serviço, como estudamos ou ainda como acompanhamos a própria saúde. De uma forma ou de outra, na grande maioria das áreas de atuação humana, somos impactados pela IA ou usamos aplicativos auxiliados por ela, os quais nos permitem ter acesso a informações ou tomar decisões de forma confiável e mais rápida do que fazíamos antes. Em função disso, novas oportunidades de trabalho surgem ligadas à tecnologia da informação como programação desses novos sistemas, análise de dados coletados, e assim, algumas profissões vão surgindo, significando boas oportunidades para alguns. Porém, em função da velocidade com que as mudanças tecnológicas chegam, o conhecimento técnico que o trabalhador tem hoje pode não lhe ser útil no ano seguinte, sendo necessário um olhar diferente para a carreira visando o aprendizado constante pois, nesse novo ambiente laboral, a única coisa permanente será a mudança. Também em função da automação de tarefas pela IA, muitos trabalhadores vão se tornar desnecessários e serão dispensados gerando um problema de desemprego em massa para muitas categorias. Alguns estudiosos e bilionários defendem a criação de um programa de renda mínima universal a ser paga para esses desempregados, já antevendo um problema mundial, com uma vasta parte da população sendo obsoleta em função das automações e melhorias trazidas pela IA. Entretanto, não está claro quem pagaria essa conta e por quanto tempo os desempregados mundiais seriam mantidos com esse possível programa social. No Brasil, ainda não há regulamentação aprovada sobre o desenvolvimento, uso e o controle da IA, o que poderia diminuir os impactos negativos para o mercado de trabalho da adoção sem limites dessa tecnologia. Em função deste cenário - envolvendo as possibilidades positivas da IA de um lado, e os grandes impactos como o desemprego em massa, de outro lado - mostra-se necessário e urgente que se aprove um marco regulatório para a IA para permitir obter bons resultados da automação, mas respeitando os direitos fundamentais do ser humano, para criar-se uma sociedade mais justa e menos desigual.

Palavras-chave: Inteligência Artificial; algoritmos opacos; discriminação algorítmica;

[1] Mestre em Direito da Sociedade da Informação (FMU-SP); Especialista em Direito de Família e Sucessões pelo IBMEC/Damásio; Bacharel em Direito (UNIP); Advogado atuando nas áreas de Direito de Família / Sucessões, Imobiliário e Contratos; MBA em Gestão Empresarial pela EAESP (FGV-SP); Especialista em Análise de Sistemas (Mackenzie); Analista de Sistemas pela FATEC-SP. Atuou como docente (Faculdades FASP) ministrando Bancos de Dados Relacionais e Modelagem de Dados para curso de Administração / Análise de Sistemas. Vice-Presidente da Comissão de Bioética e Biodireito da 38ª. subseção OAB Santo André/SP. Autor de artigos jurídicos e acadêmicos em revistas especializadas e com publicações de capítulos de livros em obras coletivas. ORCID: https://orcid.org/0000-0003-3881-1864. Lattes: http://lattes.cnpq.br/7222301214763620. E-mail: phillfernandes@philfernandes.adv.br.

desemprego pelo uso de IA; regulamentação da IA.

Abstract: Artificial intelligence (AI) is increasingly present in everyone's daily lives, impacting on the way we get news, how we research and compare product prices, how we commute to work, how we decide to hire a service, how we study or even how we monitor our health. In one way or another, in most areas of human activity, we are impacted by AI or use AI-assisted applications, which allow us to access information or make decisions more reliably and quickly than before. As a result, new job opportunities have arisen linked to information technology, such as programming these new systems, analyzing the data collected, and so some new jobs are emerging, meaning good opportunities for some. However, because technology changes speed, the technical knowledge a worker has today may not be useful in the following year, so it is necessary to take a different look at their career to constantly learn, because in this new working environment, the only thing that will be permanent is change. Also, due to the automation of tasks by AI, many workers will become unnecessary and will be laid off, creating a problem of mass unemployment for many categories. Some experts and billionaires are advocating the creation of a universal minimum income program to be paid to the unemployed, already foreseeing a worldwide problem, with a vast part of the population being made obsolete by the automation and improvements brought by AI. However, it is not clear who would pay this bill and for how long the world's unemployed would be maintained with this possible social program. In Brazil, there is no approved regulation on the development, use and AI control, which could reduce the negative impacts for the job market of the unlimited adoption of this technology. Due to this scenario - involving the positive possibilities of AI on the one hand, and the major impacts such as mass unemployment on the other - it is necessary and urgent to approve AI regulatory legislation to obtain the best results provided by automation, but respecting the fundamental rights of human beings, to create a fairer and less unequal society.
Keywords: Artificial Intelligence**;** unclear algorithms; algorithmic discrimination; unemployment due to the use of AI; AI regulation.

INTRODUÇÃO

A inteligência artificial (IA) vem se consolidado como uma das mais poderosas ferramentas tecnológicas dos últimos tempos, e está presente em nossas vidas muito mais do que imaginamos. E esse estágio atual é resultado do aumento da capacidade de processamento dos computadores à medida em que grandes volumes de dados pessoais eram coletados (big data) e processados, permitindo entender as preferências dos usuários e predizer possíveis comportamentos futuros destes usuários.

Atualmente, a automação se encontra em maior ou menor grau em todas as áreas de atuação humana, envolvendo desde monitoramento da saúde com *gadgets* específicos como *smart watches, smart rings, smart glasses*, assistentes pessoais em casa, acompanhamento da lista de compras pela geladeira inteligente e até o entretenimento com sugestões de filmes, shows etc. baseados nas preferências e interações anteriores dos usuários. Ou seja, seu

comportamento passado conta muito sobre você e sobre suas preferências e assim, isto servirá de base para que produtos e serviços de tipo igual ou semelhante lhes sejam oferecidos.

Com o aumento da capacidade computacional e o desenvolvimento de algoritmos avançados, a IA tornou-se onipresente na vida de todos, na forma de assistentes virtuais ou em diagnósticos médicos de forma preventiva, que predizem, com elevado grau de certeza, a possibilidade de alguém vir a desenvolver uma doença de acordo a análise de sua carga genética e/ou em hábitos de vida. E isto pode ser celebrado como um ponto positivo dessa "invasão de privacidade consentida" pois permite o tratamento preventivo de certas doenças e esses tratamentos médicos trazem melhores resultados aos pacientes do que os aplicados quando a doença já se encontra instalada ou em estágios avançados.

Contudo, à medida que as pessoas se tornam cada vez mais dependentes da IA, surgem também desafios a serem regulados como a coleta e o uso de dados pessoais por terceiros e os prejuízos com o vazamento desses dados, implicando em questões de elevada importância como a perda da privacidade e da liberdade individual. De outro lado, temos os impactos no mercado de trabalho gerados pela grade velocidade das transformações implementadas nas empresas com a substituição de mão-de-obra humana pela automação. Afinal, o conhecimento técnico está constantemente sendo substituído em função dessas mudanças e, assim, para o "profissional do futuro" importarão menos as capacidades técnicas que ele possui do que as habilidades comportamentais como a resiliência e a habilidade de aprender, desaprender e aprender outras coisas num processo de constante transformação pessoal. Assim, este aprendizado contínuo deverá ser um mantra em breve.

Um ponto de atenção é que, apesar de seu potencial transformador, a IA levanta preocupações éticas e sociais, especialmente quando se considera o risco de algoritmos reproduzirem vieses e preconceitos sociais com os quais foram programados, ou mesmo quando se observa o impacto da possível substituição de mão-de-obra em algumas profissões. Nesse contexto, a regulamentação da IA é um passo necessário para garantir que seu uso esteja alinhado com o respeito aos direitos humanos e aos princípios democráticos, permitindo que todos tenham voz e tenham vez.

Este artigo objetiva analisar a dependência da sociedade em relação à tecnologia e em especial à IA, e mostrar alguns riscos do uso dessa tecnologia em função dos preconceitos embutidos na criação de algoritmos, abordando, assim, a necessidade de uma supervisão por

humanos dos resultados apresentados pela IA aos usuários. Traz ainda uma visão dos impactos do uso da IA no mercado de trabalho como o desemprego para determinados setores e a criação de outros campos de atuação para os profissionais do futuro. E em função de todo este cenário, analisa a necessidade e premissas para a criação de uma regulamentação nacional para o setor de IA abordando algumas diretrizes da legislação europeia aprovada em 2024.

Para este artigo usou-se o método dedutivo com pesquisa bibliográfica e documental sobre o tema analisado. A pesquisa bibliográfica envolveu o levantamento de livros, revistas, artigos científicos, matérias publicadas na *Internet* e demais fontes documentais disponíveis; e na pesquisa documental jurídica, levantou-se a legislação em vigor no Brasil e na Europa.

1. A DEPENDÊNCIA DA INTELIGÊNCIA ARTIFICIAL E OS RISCOS

A IA vem se tornando cada vez mais presente no dia a dia de milhões de pessoas, quer através da utilização de assistentes virtuais como Siri, Alexa e Google Assistente, ou pelos resultados dos sistemas de análise de crédito usados por bancos e agentes financeiros ou mesmo na seleção de candidatos a vagas de emprego por exemplo (RUSSEL; NORVIG, 2020).

Contudo, essa dependência crescente pode trazer efeitos negativos, especialmente quando as pessoas não conhecem a lógica e o tipo de treinamento recebido pela IA, chamada de "opacidade do algoritmo" por Cathy O'Neil (2020) e tornam-se passivas diante das recomendações e decisões recomendadas pelo sistema. De acordo com Obermeyer *et al*. (2019), os sistemas de IA, quando treinados com dados históricos distorcidos ou preconceitos, tendem a repetir essas desigualdades nos resultados. É o que, na Tecnologia da Informação, é conhecido como o princípio do "*garbage in – garbage out*", algo como "entra lixo (dados ruins), sai lixo (resultados ruins) em tradução livre.

E isso tem uma enorme importância quando esses algoritmos opacos produzem resultados estranhos para definir a alocação de recursos públicos em setores como escolas, saúde ou na área de segurança pública de uma cidade, por exemplo.

Além de dados incorretos, os algoritmos de IA podem reproduzir preconceitos de diversos tipos analisando atributos como local de nascimento, gênero, etnia, nível de escolaridade e usar esses atributos com efeito de segregação ou com base nesses dados apontar quem tem mais chance de cometer um crime ou de inadimplir um empréstimo num banco. Um exemplo disso, foi o estudo de Buolamwini e Gebru (2018), onde um sistema de

reconhecimento facial falhou ao não conseguir identificar pessoas pretas e asiáticas, pois a programação foi feita usando apenas rostos de pessoas brancas. Falhas desse tipo, se não forem corrigidas de imediato podem reforçar estereótipos e marginalizar ainda mais os grupos já discriminados na sociedade.

Essa dependência de sistemas de IA também tem efeitos psicológicos graves. Como Zuboff (2019) demonstra, ao permitir que a IA tome decisões em uma escala tão ampla, a sociedade corre o risco de perder autonomia e de ver suas escolhas influenciadas e moldadas por empresas de tecnologia e governos, muitas vezes sem transparência ou controle sobre os dados usados para essas decisões.

A pesquisa de Zuboff aborda a lógica do capitalismo de vigilância e se detém em quatro pilares, dos quais destacamos dois mais relacionados com o exposto acima. O primeiro pilar é o objetivo de personalização dos serviços oferecidos para os usuários de plataformas digitais, o que necessita da obtenção de dados (com ou sem consentimento do usuário) e do uso de *cookies* de rastreamento que a maioria dos sites impõe como única forma de ter acesso aquele site ou àquela solução. Apesar de haver legislação específica para proteger os usuários - no Brasil temos a LGPD, Lei no. 13.709/2018 - ainda são raros os casos de plataformas que permitem a navegação sem condicionar à aceitação de *cookies*.

O segundo pilar envolve o uso de infraestrutura tecnológica para executar experimentos futuros com os usuários e consumidores. Isto se verifica nos “Termos de Aceite” que a solução apresenta ao usuário e que quase ninguém lê. Esses “Termos de Aceite” normalmente preveem “autorização explícita e ampla” para a solução usar os dados do internauta, o que é feito com um singelo “x” num formulário eletrônico. E preveem ainda o compartilhamento dos dados coletados com “empresas parceiras”, as quais o usuário não sabe quem são e nem como os dados dele serão usados, por quanto tempo, com qual finalidade e como e quando serão descartados.

Outro risco significativo da dependência da IA está nos tipos de algoritmos utilizados em decisões de alto impacto, como avaliações de crédito, contratações de financiamento imobiliário e acesso a seguros. Segundo Cathy O'Neil (2020), algoritmos baseados em dados históricos podem reforçar desigualdades preexistentes, operando de forma opaca e sem a supervisão adequada. Ela aponta que esses sistemas, que deviam ser imparciais, na verdade, reproduzem preconceitos e discriminações embutidos nos dados. Por exemplo, algoritmos que

analisam a pontuação de crédito para conceder empréstimos pessoais podem penalizar certos grupos sociais ou moradores de determinada região do país ou da cidade, criando barreiras financeiras para comunidades já desfavorecidas.

Na proposta de crédito que é preenchida, o interessado informa o endereço e CEP e com esta informação, algumas tabelas de dados são consultadas para ver a adimplências dos pagamentos pelos moradores daquela região e dali inferir como o interessado deverá agir com relação à pontualidade do pagamento do empréstimo dele. Ou seja, do comportamento do grupo deduz-se o comportamento do indivíduo, e isso pode ter um peso maior do que o histórico pessoal daquele indivíduo quanto ao seu passado de adimplemento de crédito.

Essa situação remete a uma teoria usada no fim do século XIX denominada determinismo social. Por essa teoria, o homem era fruto do meio em que vivia e as estruturas sociais determinavam a ação dos indivíduos, enquanto as condições sociais determinavam o comportamento das pessoas. E desta forma, os indivíduos que compartilhavam da mesma estrutura cultural (vivendo numa mesma localidade) tenderiam a pensar e agir de forma semelhante. Porém, essa teoria mostrou-se inadequada pois condenaria os que nascem em locais marginalizados a serem marginais e sem possibilidades de romper esse "destino".

Além disso, O'Neil (2020) descreve esses algoritmos opacos como "armas de destruição em massa" justamente porque operam em larga escala e afetam vastos grupos populacionais, aumentando as desigualdades e deixando poucas opções para os indivíduos corrigirem as injustiças. O processo é especialmente problemático, pois os algoritmos não consideram as nuances individuais e utilizam variáveis de contexto que muitas vezes fogem ao controle dos afetados. Essa falta de transparência e o caráter de uma "caixa-preta" dos algoritmos tornam difícil a contestação e a identificação de discriminações, gerando impactos negativos para a justiça social e para o equilíbrio democrático (O'NEIL, 2020).

Portanto, os riscos de discriminação algorítmica são mais presentes do que se supõe e nas análises de Cathy O'Neil, a dependência da IA de forma total, sem questionamentos, sem regulamentação ou até sem supervisão humana levam a consequências graves como a restrição de direitos e liberdades individuais.

2. A IA, O DESEMPREGO E O PROFISSIONAL DO FUTURO

A era da Inteligência Artificial (IA), neste momento, recebe um grande destaque em várias áreas de negócios e, apesar da efervescência, ninguém sabe ao certo até onde ou para onde ela nos levará. A euforia e a apreensão iniciais devem passar e haverá a seleção normal deixando no mercado apenas os modelos que podem gerar bons resultados práticos. E isso pode-se verificar quer seja em aplicações comerciais, voltadas para a área de saúde, de segurança ou mesmo de entretenimento. Ao final, o que irá importar é o quanto a solução com a IA pode colaborar para o incremento dos negócios.

Conforme o relatório *The economic potential of generative AI: the next productivity frontier* produzido pela *McKinsey Global Institute*, num cenário otimista, a IA generativa pode injetar USD 4,4 trilhões (CHUI, 2023) por ano na economia mundial, e quase metade dos trabalhos humanos poderão ser automatizados entre 2030 e 2060 (LOPES, 2023), o que traz apreensão para muitos e oportunidades para outros.

Esta substituição da mão-de-obra por sistemas automatizados não é um privilégio ou um risco criado pelo *boom* da IA, visto que isso se deu com as Revoluções Industriais anteriores a esta, tida como a Quarta Revolução. Nesta, vemos uma combinação do uso massivo da *Internet*, de dispositivos (*gadgets*) impactando na *Internet* das coisas (*IOT*) alimentada e alimentando múltiplas soluções de IA.

O site *there's an IA for that* (*https://theresanaiforthat.com*) cataloga soluções de IA desenvolvidas desde 2015, envolvendo soluções gratuitas ou pagas e, para o período de janeiro a junho de 2023, registrou o lançamento de 1086 soluções de IA (*https://theresanaiforthat.com/timeline*), indicando mais de uma nova ferramenta lançada por dia. Para comparação, em todo o ano de 2021, foram lançadas 252 soluções e no ano de 2022, houve 621 soluções novas.

Esse aumento faz parte da etapa de deslumbramento que ocorre com o lançamento de novas tecnologias que têm seu *boom* com muita divulgação e adoção em grande escala como se fossem a solução para todos os anseios da humanidade, mas que tempos depois são colocadas no devido lugar sobrando aquelas que, de fato, conseguem trazer resultados significativos para as empresas e usuários.

Entretanto, ainda estamos na fase da euforia, em que o lançamento de aplicações não para de crescer. No próprio site citado, é possível inscrever-se para receber a *newsletter* sobre o mercado de IA, e essa *newsletter* é produzida por outra IA. Conforme o site: "*Escrita pelo*

ChatGPT. A maior base de dados de IA. Nunca perca outra IA. Nós estamos lançando nossa exclusiva newsletter, escrita pelo ChatGPT. Assine abaixo e iremos adicionar você me nossa lista de espera" numa tradução livre.

O mais curioso é que ao se inscrever para receber a *newsletter,* o usuário recebe um e-mail com o texto: "Para ter certeza de que você não é um robô e que nossos futuros e-mails possam ser recebidos por você, poderia, por favor retornar este e-mail com "IA"? Isto realmente nos ajudaria!" numa tradução livre. Assim, uma IA requer a um humano para confirmar que ele é um humano para ela poder disparar um processo em que outra IA irá gerar uma *newsletter* personalizada de acordo com as preferências desse humano.

Segundo a teoria da destruição criativa de Joseph Schumpeter (1942), as transformações na sociedade não ocorrem de forma linear, mas sim através de grandes ciclos e rupturas que são impulsionadas pelas inovações tecnológicas. A "destruição criativa" é um conceito no qual o autor descrevia uma mudança no perfil econômico, onde os empreendimentos inovadores destruíam empresas e modelos de negócios antigos e ultrapassados (SILVA, 2019) e em seu lugar outros eram criados.

Este processo não é novidade e já se verificou na 1ª. Revolução Industrial, depois com a chegada da eletricidade, com os automóveis, além da era da informática e *Internet*. Desta forma, algumas ocupações são substituídas por processos automatizados ou por robôs, como ocorreu de forma expressiva na automação das montadoras de automóveis nos anos 80 e 90. Naquele momento, áreas inteiras que tinham muitos empregados passaram a ter apenas robôs em suas atividades e o elemento humano passou a ser usado apenas se havia necessidade de intervenção em alguma das máquinas.

Assim, o progresso mostra-se cíclico e de tempos em tempos, uma nova onda surge destruindo ou substituindo o que era o padrão por algo novo e apoiado em mais tecnologia e diminuindo a dependência da mão de obra humana. Assim, certas atividades laborais deixam de existir, levando seus profissionais a buscar outras possibilidades de trabalho.

A título de exemplo, podemos citar o impacto que a chegada dos smartphones trouxe ao mercado em geral. De uma hora para outra, não fez mais sentido ter-se de forma separada dispositivos como uma câmera digital, uma calculadora, um gravador de voz, um telefone celular, um tocador de *mp3*, um dicionário ou um tradutor de idiomas. O *smartphone* inovou pois oferecia essas funcionalidades e outras num único equipamento, tornando-se uma

ferramenta essencial para qualquer profissional que precisava se comunicar com seus clientes, fornecedores e parceiros de negócios. Além desses vários *gadgets*, o *smartphone* também aposentou e incorporou as agendas e os guias de ruas e endereços que eram em papel, tornando-se também digitais.

Neste caso, o mercado que produzia e vendia os dispositivos citados, num primeiro momento perdeu, mas em paralelo, uma nova indústria se criou com desenvolvimento de *Apps*, *games*, soluções de *streaming,* dispositivos *wearables* dentre outros. Com isso, todos foram impactados e cada vez mais circundados e dependentes da tecnologia, da *Internet* e de assistentes digitais para as atividades e tarefas rotineiras usando *Alexa* (da *Amazon*)*, Siri* (da *Apple*)*,* e *Ballie* (da *Samsung*)*,* dentre outras, sendo esta última, a mais recente no mercado.

Em 2018, um caso muito interessante foi apresentado pelo *CEO* da Google, Sundar Pichai, num evento da empresa, onde a assistente da Google, nomeada de *Duplex*, efetuou ao vivo uma chamada telefônica a um salão de beleza para marcar um horário para corte de cabelo feminino (VENTURA, 2018). A assistente conseguiu simular muito bem o comportamento humano utilizando a tecnologia de compreensão de linguagem natural ao ter que lidar com alternativas de horário e de possíveis serviços oferecidos pela atendente do salão e, ao final, a *Duplex* escolheu um serviço e horário que se "ajustavam na agenda dela" (YOUTUBE, 2018).

Assim, é previsível que vários postos de trabalho deixem de existir, num primeiro momento afetando atividades mais repetitivas ou burocráticas. Porém, até mesmo as atividades intelectuais e que exigem criatividade e sensibilidade serão afetadas. Basta verificar experimentos feitos na área artística, onde o robô ROBOTOR usando sete eixos de trabalho e auxiliado por uma IA consegue reproduzir obras-primas de grandes mestres da escultura feitas em mármore Carrara sem os inconvenientes problemas que ocorrem com humanos. O robô não causa danos ao bloco de mármore por imprecisão no uso das ferramentas, nem inala pó de mármore, o que diminuiria a velocidade de execução da peça, não precisa de parada para alimentação ou repouso e nem exige elevado salário para executar a obra (CUNHA, 2022).

Ocorre que a velocidade de extinção de certas atividades profissionais é bem maior do que a velocidade de surgimento de novas oportunidades, quer seja através da requalificação profissional dos que já estão no mercado (vindos de um mundo analógico) ou mesmo na criação de funções para aqueles que estão ingressando no mercado de trabalho. E é nesse intervalo de tempo que os maiores desafios devem surgir, pois o processo de requalificação não é algo que

ocorre de forma rápida e nem é uniforme para os que forem alijados de seus postos de trabalho.

Em primeiro, devido às particularidades de cada ser humano: conhecimento técnico para o novo aprendizado, facilidade de transição e de adaptação à nova realidade dentre outros fatores. O que já deixa antever que uma parte significativa dos profissionais dispensados não conseguirá se encaixar no novo cenário profissional, podendo impactar na necessidade de criação ou extensão de programas sociais temporários do governo para auxiliar a esses trabalhadores dispensados que não conseguiram se requalificar.

Em segundo lugar para os que conseguirem se requalificar, haverá a competição não só com seus iguais - vindos de um mundo analógico - mas também com profissionais mais novos e que já nasceram num mundo totalmente digital e, para estes, o uso constante e a dependência de sistemas baseados em IA e em *Internet* das coisas (*IOT*) serão fatos banais. Portanto, é de se esperar que os mais jovens tenham desempenho superior à maioria dos mais velhos, o que poderá resultar numa 2ª. onda de expurgo desses profissionais, agora em doses mais homeopáticas e "assimiláveis" pela sociedade da informação.

Assim, será necessário requalificar os profissionais que hoje desempenham papéis mais operacionais e que tendem a ser substituídos por processos automatizados ou baseados em IA, mas isso não é tudo. Os riscos da automação podem ser vistos como boas oportunidades de crescimento profissional para aqueles dispostos a se requalificarem para atividades novas e mais necessárias com o uso da IA em grande escala.

Fica evidente que os mais afetados por essa mudança serão aqueles com menor qualificação e com baixos salários, e por serem em grande número pode-se antever um desemprego em larga escala, afetando o mundo como um todo (SCHNEIDER, 2018).

Alguns sindicatos têm-se movimentado fazendo pesquisas junto a empregados para analisar possíveis riscos de empregabilidade ou até detectar a já existência do problema numa categoria. Isso está sendo feito também junto aos empregadores para identificar planos de automação de processos pelo uso da IA e possível demissão de vários profissionais.

Um dos exemplos ocorreu com o SEPROSP – Sindicato das empresas de Processamento de Dados e serviços de Informática do Estado de São Paulo que lançou a pesquisa de avaliação "O impacto do Uso da IA Generativa no mercado de Trabalho"

Na página do sindicato na *Internet* verifica-se:

> Em um cenário de transformação digital acelerada, a **IA Generativa** emerge como uma tecnologia disruptiva com o potencial de remodelar profundamente as relações

> de trabalho. Diante desse contexto, este projeto de pesquisa aprofundada visa analisar criticamente como a implementação da IA pode afetar tanto os trabalhadores quanto os ambientes de trabalho. (SEPROSP, 2024).

A pesquisa está em andamento e os resultados devem ser divulgados até o final de 2024.

Em decorrência deste cenário, algumas questões de alta relevância e pontos de reflexão são trazidos a seguir:

- Afinal, quais serão essas profissões do futuro e como os mais jovens devem se preparar para elas?
- Sem considerar o aumento populacional do planeta, haverá espaço no mercado de trabalho para absorver profissionais de qualificação mediana em termos tecnológicos e com 20 anos ou mais de experiência em atividades que não mais serão necessárias?
- Se essas pessoas tiveram pouco acesso a estudo, e por isso, obtiveram posições mais operacionais, como elas poderão se preparar para novos desafios que exigirão uma qualificação bem mais elevada e muito estudo?
- Para resolver ou amenizar isso, a criação de programas sociais de renda mínima destinada a esses trabalhadores seria uma solução?

Ocorre que o problema não fica restrito ao cenário nacional, visto que o desemprego deverá ser transnacional. E assim, fica a questão: como os países mais pobres podem lidar com esse problema? Afinal, a automação gerada pela IA deverá trazer impactos para todos os países ou para a grande maioria. Neste cenário, qual seria a participação dos países mais desenvolvidos para resolver o problema, visto que reduzirão a necessidade de mão de obra dos países pobres?

Se a solução for a criação de um programa de renda mínima, como defende Sam Altman, CEO da *OpenAI,* controladora do ChatGPT, e Ellon Musk, *CEO* da *Tesla, Inc*. (EMERSON, 2024), como definir qual será esse mínimo, tendo em vista a dignidade humana e a desigualdade existente entre os países?

E, afinal, quais serão esses empregos do futuro? De acordo com a Comissão Econômica para a América Latina e Caribe (CEPAL), 65% das crianças que entram hoje no ensino fundamental, terão empregos que ainda não existem. Alicia Barcena, diretora da CEPAL, defendeu a necessidade de criação de políticas educacionais para acompanhar o desenvolvimento sustentável, afirmando que: “Precisamos ajudar os jovens a compreender as

novas tecnologias porque muitos empregos que existem hoje não existirão no futuro. Estamos preparando pessoas para trabalhos que não existirão" (NAÇÕES UNIDAS BRASIL, 2018).

Apesar de não se saber quais serão as profissões do futuro, pode-se antever as características do profissional dessa nova era. O profissional do futuro estará vinculado ao desenvolvimento e bom uso de suas capacidades comportamentais, visto que, num mundo dominado pela tecnologia, o conhecimento técnico terá duração muito curta, devido à rápida e constante mudança da tecnologia.

Ocorre que nossa sociedade está criando inúmeras soluções de IA, mas não está capacitando os profissionais a lidarem de forma adequada com a inteligência emocional para lidar com essas mudanças. E isso fará toda a diferença num mundo circundado por máquinas apoiadas pela IA e profissionais que terão que se reinventar continuamente para manterem-se atualizados e necessários.

Desta forma, flexibilidade de aprendizagem, competência ao utilizar a inteligência emocional, capacidade de resolver problemas complexos, além de habilidade em negociação e liderança serão atributos mais importantes do que ter o domínio da ferramenta A ou B, em função da rapidez de obsolescência dessa parte técnica.

Para Alvin Toffler, o analfabeto do século XXI não será aquele que não consegue ler ou escrever, mas aquele que não consegue aprender, desaprender e reaprender (EXAME, 2019). E segundo estimativas de experts em comportamento humano e vida laboral, um profissional dos próximos anos poderá ter até cinco carreiras na sua trajetória de trabalho, podendo até virem a acontecer ao mesmo, conforme explica Michelle Schneider, do Linkedin. Portanto, nesse cenário, a única coisa que será permanente é a mudança, visto que o ato de reaprender será uma atividade constante na vida profissional.

3. A IA E A FALTA DE DIRETRIZES OU DE LIMITES

Conforme já comentado, são lançadas por dia em torno de cinco soluções tecnológicas baseadas em IA e os volumes de novas ferramentas vem aumentando ano após ano. Ocorre que pela grande velocidade de lançamento e de adesão a estas soluções, ainda não se conseguiu definir normas claras para limites que a IA deve respeitar, deixando dúvidas sobre quais são os protocolos de segurança usados em cada IA, a qualidade dos dados utilizados no treinamento da solução, os preconceitos e vieses embutidos na programação inicial, bem como a definição

das etapas e procedimentos de aprendizagem pela IA quando em produção com a coleta de um grande volume de dados.

Assim, vemos dois momentos críticos onde deve haver transparência: na definição das regras de programação inicial da ferramenta, e na fase de seleção, análise e descarte de novos dados durante a etapa de aprendizagem quando esses dados reforçam estereótipos, misoginia, preconceitos e outras formas de segregação. Porém, ao invés das regras de construção da IA serem abertas, o que temos é que "modelos opacos e invisíveis são a regra, e os transparentes a exceção" (O'NEIL, 2020).

Lembrando que essa discriminação pode ocorrer por origem social, gênero, por origem geográfica, etnia, renda etc. Caso essa segunda fase - de aprendizagem - não seja muito bem acompanhada por elementos humanos e seja possível de auditar, teremos um grave problema. Isso porque, ainda que a programação inicial não tenha determinados comportamentos e parâmetros de segregação, a fase de *machine learning* necessita de mecanismos de valoração adequada dos novos dados coletados, o que deve ser feito com a intervenção humana através de mediadores para auxiliar na triagem, a chamada "supervisão humana".

A título de exemplo da situação descrita, em 2016 houve o lançamento do *bot* da *Microsoft* denominado "Tay" que deveria interagir de forma quase humana com os usuários, usando uma linguagem quase natural. Porém no dia de seu lançamento, ela passou a receber muitas mensagens de cunho sexista, antissemita e de xenofobia vindas de usuários do *Twitter* (atual X) e num processo mal gerenciado de aprendizagem, ela entendeu que aquilo era um comportamento natural dos seres humanos, incorporou isso e passou a reproduzir esse comportamento em suas novas respostas aos usuários. (CANO, 2016).

A Tay foi criada para atuar com público jovem, na faixa de 18 a 25 anos, mas não conseguiu entender piadas de mau gosto, afirmações de que o Holocausto nunca aconteceu ou afirmações de que a mulher é a escória da humanidade, e acabou incorporando tais "dados" como verdadeiros em seu repertório e passou a ter esse tom nas próximas interações com os usuários. Afinal, a Tay não sabia entender frases ditas em tom de ironia ou mesmo avaliar que mentiras contadas por pessoas diferentes não se tornam verdades.

Os técnicos da Microsoft perceberam a incapacidade da Tay em sopesar as informações recebidas, filtrá-las e descartar as de cunho segregacionista, e optaram por desligá-

la no mesmo dia de seu lançamento. Esta situação demonstra os desafios éticos e técnicos na criação de IA que aprende a partir de todo tipo de dados não supervisionados.

Porém, como na *Internet* não há direito ao esquecimento, ainda hoje é possível ter acesso a várias mensagens inadequadas da Tay que foram gravadas por usuários em https://socialhax.com/2016/03/24/microsoft-creates-ai-bot-internet-immediately-turns-racist/. Uma das frases que chamou a atenção foi "*Stop deleting the genocidal Tay tweets @Microsoft, let it serve as a reminder of the dangers of AI - ON THE RUN BOOGYMAN (@DetInspector) March 24, 2016*". Algo como "Microsoft, pare de apagar as mensagens da Tay sobre genocídio (holocausto) e deixe isso servir de lembrete sobre os riscos da IA" numa tradução livre (SOCIALHAX, 2016).

Apesar do acontecido em 2016, a falta de regulamentação do uso da IA ainda permanece e em função da maior quantidade de soluções utilizando-se da IA atualmente, os riscos de efeitos nocivos aumentaram de forma significativa.

A discriminação algorítmica mostra-se presente também no processo de seleção e recrutamento para vagas a serem preenchidas em uma empresa, na qual "Um programa de computador poderia vasculhar milhares de currículos ou pedidos de empréstimo em um segundo ou dois e ordená-los em listas impecáveis, com os candidatos mais promissores no topo" (O'NEIL, 2020).

Aqui, vemos que a subjetividade e a experiência de um bom recrutador na análise de um *curriculum* não é algo inerente a um algoritmo e, de outro lado, os critérios utilizados pelo algoritmo para definir a pontuação dos candidatos não são transparentes, sendo que os algoritmos têm em sua programação, em maior ou menor grau: preconceitos, equívocos e vieses humanos que comprometem uma análise feita de forma imparcial.

Considerando isto, a velocidade e quantidade de lançamentos de soluções baseadas em IA, mostra-se urgente a necessidade de regulação da IA nas fases de pesquisa, desenvolvimento da solução, bem como na aprendizagem de máquina com dados coletados e na seleção e valoração desses dados. A IA não tem consciência nem condições de atribuir juízo de valor aos dados e premissas com que foi programada, sendo necessária uma validação por elementos humanos que podem atuar como supervisores da IA para evitar ou diminuir os resultados não desejados.

Ocorre que os desenvolvedores de soluções de IA não observam fronteiras geopolíticas

pois não têm necessariamente sede nos principais centros comerciais onde operam, e assim, a coleta de dados pode ocorrer num país, e seu uso para treinamento das soluções ser feito em outro local com legislação de proteção de dados diferente. E isto pode trazer prejuízos aos usuários, devido às limitações do alcance jurisdicional de cada nação e à forma como o Direito opera atualmente. Por isso, mais do que se definirem parâmetros para a criação de uma regulação local, é necessário trabalhar-se para que haja uma harmonização global dessa regulação, visto que o que temos até agora são recomendações como a da OCDE de 2019[2] e da UNESCO[3] de 2021. E por se tratar de *soft law*, são de adesão facultativa e sem o condão de aplicação de sanções aos infratores (BARROSO, 2024. P. 50-51).

Nessa linha de buscar-se uma uniformidade de regulação, em 2023, mais de mil pesquisadores, cientistas e empresários (Ellon Musk dentre eles) assinaram uma carta aberta pedindo uma pausa de, pelo menos 6 meses, no desenvolvimento de soluções de IA até que protocolos de segurança fossem desenvolvidos, implementados, compartilhados e auditados por especialistas independentes (COELHO, 2023). Porém, a corrida continuou de forma frenética pois - apesar das demandas por governança, regulação, monitoramento, e atenção para os impactos sociais, econômicos e políticos das novas tecnologias - "os avanços na área se tornaram objeto de disputa entre nações, pesquisadores e empreendedores" (BARROSO, 2024, p. 49). Afinal, os negócios não podem parar, pois tempo é dinheiro, conforme qualquer capitalista.

4. A REGULAÇÃO APROVADA NA UNIÃO EUROPEIA E SEUS IMPACTOS NO BRASIL

Em marco de 2024, a União Europeia (UE) aprovou o *Artificial Intelligence Act* para definir regras mais claras sobre o desenvolvimento, a implantação e a operação da IA, e nesta regulamentação estão as regras e as penalidades para aqueles que não seguirem a norma legal. E um ponto que deve ser ressaltado é que as penalidades são proporcionais ao nível de risco para as pessoas ou bens afetados pela IA.

A norma europeia classifica as possibilidades da IA em três níveis de riscos

[2] OCDE = Organização para a Cooperação e Desenvolvimento Econômico. Em 2019 lançou a Recomendação do Conselho sobre Inteligência Artificial.
[3] UNESCO = Organização das Nações Unidas para a educação, Ciência e Cultura. Em 2021 lançou a Recomendação sobre Ética na Inteligência Artificial.

envolvidos: i) um risco inaceitável, ii) um risco elevado, iii) um risco baixo ou mínimo. A lista de práticas proibidas (riscos inaceitáveis) encontra-se no Título II do documento e incluem todos os sistemas de IA cuja utilização seja considerada inaceitável por violar os valores da UE como, por exemplo, violar os direitos fundamentais. Incluem-se nessa restrição aplicações com potencial significativo para manipular crianças ou pessoas com deficiência para distorcer substancialmente o seu comportamento, podendo causar danos psicológicos ou físicos a si ou a outra pessoa. (EUROPEAN UNION, 2024).

Já as soluções de IA que apresentem risco elevado, estas só podem ser lançadas caso não representam riscos inaceitáveis para interesses públicos da UE ou se cumprirem determinados requisitos obrigatórios e definidos pela UE. Nesta categoria podemos ter aplicações relacionadas ao controle de tráfego numa cidade, ao abastecimento de água e eletricidade, ou no uso de dados biométricos de indivíduos, dentre outros.

No Brasil, temos dois projetos de lei (PL) tratando do tema de regulação da IA: o PL 2339/2023 e o PL 21/2020, e pelo estágio de ambos e em função da aprovação da regulação da UE é bastante natural que haja uma forte influência desta sobre os dispositivos locais, a exemplo do que aconteceu com a aprovação da LGPD (Lei no. 13.709/2018) que remeteu à similar regra europeia RGPD aprovada em abril de 2016.

De toda a forma, em função da importância do tema, da influência que os mecanismos de IA têm sobre a vida das pessoas e da atual falta de limites e diretrizes para o desenvolvimento de soluções tecnológicas baseadas em IA, além da possibilidade de uma crise de desemprego em escala mundial, fica evidente a necessidade de se aprovar no país, um marco regulatório da IA. E, em linhas gerais, este deve garantir que os direitos humanos e, em especial, os direitos fundamentais não sejam violados; que haja regras claras dos tipos de finalidades da IA que não poderão ser exploradas: aquelas aplicações que apresentem riscos inaceitáveis para a sociedade; e por fim que as empresas de desenvolvimento de tais tecnologias sejam responsabilizadas de forma proporcional aos danos causados aos usuários.

Em termos de diretrizes a serem seguidas, a regulação que vier a ser aprovada deve contemplar o benefício dos seres humanos, diminuindo a exposição destes a riscos, e seguir três pilares: (BARROSO, 2024, p. 53-57).

a) <u>defesa dos direitos fundamentais</u>, atuando sobre a privacidade da informação: onde o uso de dados pessoais ou corporativos não possa ser feito sem o prévio e

esclarecido consentimento de seus detentores. A não discriminação algorítmica deve ser garantida a todos; e a autonomia individual deve ser preservada através do direito à liberdade e à informação;

b) a proteção da democracia garantindo que todos tenham voz deve ocorrer através do combate à desinformação (*fake news*), aos discursos de ódio, e aos ataques às instituições democráticas; e

c) a promoção da boa governança projetada para garantir o bem-estar social em um meio ambiente saudável: feita com a participação do poder público, pesquisadores, entidades defensoras dos direitos humanos, e sociedade civil. A transparência e explicabilidade dos algoritmos e dos resultados trazidos por estes deve ser regra para permitir questionamentos por aqueles que se julgarem prejudicados. Especial atenção deve ser dada à segurança dos algoritmos quanto a ataques externos, à análise de impactos e à qualidade dos dados utilizados. E por fim, a existência de supervisão humana para que a IA opere dentro da legalidade, da ética e da justiça.

CONCLUSÕES

A IA está mudando a sociedade atual de uma maneira profunda, trazendo benefícios mas também deixando-a diante vários problemas como a crescente dependência das tecnologias - resultado da sociedade da informação - e os riscos daí advindos, especialmente pelo uso de dados pessoais, a invasão da privacidade dos indivíduos, além da discriminação algorítmica gerada pela falta de transparência dos critérios usados pelos aplicativos baseados na IA.

Além disso, há vários riscos associados à automação de processos sem limites para o uso da IA e estes devem impactar no mercado de trabalho levando à extinção em massa de vários postos de trabalho. E esta situação exige uma resposta rápida e deve ser construída ouvindo-se os diversos participantes da sociedade como o poder público, empresas, sindicatos e entidades defensoras dos direitos humanos. Uma das possíveis soluções envolve a criação de políticas públicas voltadas a auxiliar essa força de trabalho dispensada para sua requalificação e o desenvolvimento de novas habilidades para sua reinserção no mercado laboral. Uma outra solução deve prever o estabelecimento de limites ao uso da IA para mitigar os impactos como demissões em massa de trabalhadores, mas essa alternativa não conseguirá ser usada por prazo

indeterminado pela pressão e importância que o mundo corporativo (empregadores) exerce no cenário atual.

De toda forma, considerando a quantidade de novas soluções baseadas em IA lançadas por dia, a elevada adesão e dependência tecnológica dos usuários dessas soluções e a não existência de legislação brasileira sobre o tema, agora é o momento para esse diálogo e busca de soluções, sob risco não conseguirmos criar uma regulação que proteja os direitos fundamentais dos indivíduos, o emprego e promova a justiça social.

A regulamentação da IA aprovada em 2024 pela União Europeia demonstra que é possível estabelecer um marco regulatório que incentive o desenvolvimento da inovação, mas que consiga atuar dentro de parâmetros éticos e que respeite a proteção dos direitos fundamentais dos indivíduos. O Brasil pode se inspirar naquela legislação para criar uma estrutura que favoreça o desenvolvimento tecnológico responsável, evitando e combatendo a discriminação e a falta de transparência dos algoritmos.

É essencial que todos os envolvidos: poder público, empresas, sindicatos e a sociedade civil trabalhem juntos para enfrentar os desafios e aproveitar as oportunidades que a IA promete trazer. A IA, como qualquer ferramenta não é boa ou má em si mesma, mas a utilização que for feita dela é que vai trazer bons ou maus resultados para a sociedade.

A IA está se mostrando uma ferramenta poderosa e se utilizada de forma ética e responsável, com controle e supervisão humana pode transformar positivamente uma sociedade trazendo melhores condições de vida. Entretanto, se não houver controle adequado sobre o desenvolvimento e depois o acompanhamento e análise dos resultados usando supervisão humana adequada, essa ferramenta pode trazer prejuízos de difícil reparação para muitos.

Assim, o compromisso com a regulação, a educação no uso das soluções criadas e o apoio à inovação devem ser prioridades na construção dessa nova sociedade, onde a tecnologia seja uma aliada do ser humano trabalhando em favor deste e ajudando a diminuir as diferenças neste mundo globalizado. Assim, poderá ser possível trazer a harmonia necessária para permitir a criação de uma sociedade mais justa e fraterna.

REFERÊNCIAS

BARROSO, Luís Roberto. **Inteligência artificial, plataformas digitais e democracia – direito e tecnologia no mundo atual**. Belo Horizonte. Ed. Fórum. 2024.

BUOLAMWINI, Joy; Gebru, Timnit. **Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification.** ***Proceedings of Machine Learning Research***. E 81, p. 1-15. 2018. Disponível em: https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf. Acesso em 18 ago. 2024

CANO, Rosa J. EL PAÍS. Tecnologia. **O robô racista, sexista e xenófobo da Microsoft acaba silenciado**. 2016. Disponível em: https://brasil.elpais.com/brasil/2016/03/24/tecnologia/1458855274_096966.html. Acesso em 18 out. 2024.

CHUI, Michael et all. MCKINSEY DIGITAL. ***The economic potential of generative AI – The next productivity frontier***. 2023. Disponível em: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/The-economic-potential-of-generative-AI-The-next-productivity-frontier#introduction. Acesso em 12 set. 2024.

COELHO, Renato. Jornal da Unesp. **Especialista em ciência da computação da Unesp analisa abaixo-assinado que pede moratória para o desenvolvimento da inteligência artificial**. 2023. Disponível em: https://jornal.unesp.br/2023/04/12/especialista-em-ciencia-da-computacao-da-unesp-analisa-abaixo-assinado-que-pede-moratoria-no-desenvolvimento-da-inteligencia-artificial/. Acesso em 12 out. 2024.

CUNHA, Roberto. Inovação para a vida. Stylo Urbano. **ROBOTOR: o robô-escultor que esculpe o mármore de Carrara!**. 2022. Disponível em: https://www.stylourbano.com.br/robotor-o-robo-escultor-que-esculpe-o-marmore-de-carrara/. Acesso em 18 out. 2024.

EMERSON, Sarah. Forbes Money. **Por que Sam Altman passou a defender uma renda mínima universal**. 2024. Disponível em: https://forbes.com.br/forbes-money/2024/07/fundador-da-openai-sam-altman-deu-dinheiro-a-milhares-de-pessoas-saiba-o-que-aconteceu/. Acesso em 23 out. 2024.

EUROPEAN UNION. **Artificial Intelligence Act.** 2024. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52021PC0206. Acesso em 22 out. 2024.

EXAME. Crescer em Rede. **Chegou a hora de você desaprender.** 2019. Disponível em: https://exame.com/colunistas/crescer-em-rede/chegou-a-hora-de-voce-desaprender/. Acesso em 20 out. 2024.

LOPES, André. EXAME. **Inteligência artificial generativa pode injetar US$ 4,4 trilhões anualmente na economia global**. 2023. Disponível em https://exame.com/inteligencia-artificial/inteligencia-artificial-generativa-pode-injetar-us-44-trilhoes-anualmente-na-economia-global/. Acesso em 12 out. 2024.

NACÕES UNIDAS BRASIL. Notícias. **Com evolução tecnológica, 65% das crianças terão**

empregos que ainda não existem, diz CEPAL. 2018. Disponível em https://brasil.un.org/pt-br/80575-com-evolu%C3%A7%C3%A3o-tecnol%C3%B3gica-65-das-crian%C3%A7as-ter%C3%A3o-empregos-que-ainda-n%C3%A3o-existem-diz-cepal. Acesso em 28 set. 2024.

OBERMEYER, Ziad., Powers, Brian., Vogeli, Christine, Mullainathan, Sendhil. (2019). ***Dissecting racial bias in an algorithm used to manage the health of populations***. Science. Research Article. V. 366 (6464). p 447–453. Disponível em: https://www.science.org/doi/10.1126/science.aax2342. Acesso em 12 out 2024.

O'NEIL, Cathy. **Algoritmos de destruição em massa: como o big data aumenta a desigualdade e ameaça a democracia**. Rio de Janeiro, Ed. Rua do Sabão. 2020.

RUSSELL, Stwart; NORVIG, Peter. ***Artificial Intelligence: A Modern Approach***. 4. ed. New York. Pearson. 2020.

SCHNEIDER, Michelle. YOUTUBE. TEDx Talks. **O profissional do Futuro**. Michele Schneider. 2018. Disponível em https://www.youtube.com/watch?v=9G5mS_OKT0A. Acesso em 16 set. 2024.

SEPROSP. Notícias. **Pesquisa Nacional sobre o impacto do uso da Inteligência Artificial.** 2024. Disponível em: http://www.seprosp.org.br/?p=4436. Acesso em 18 out. 2024.

SILVA, Lúcio de S. VIA UFSC. **Schumpeter: desenvolvimento por meio da inovação.** 2019. Disponível em: https://via.ufsc.br/schumpeter-inovacao/#:~:text=A%20destrui%C3%A7%C3%A3o. Acesso em 18 set. 2024.

SOCIALHAX. **Microsoft Creates AI Bot – Internet Immediately Turns it Racist**. 2016. Disponível em: https://socialhax.com/2016/03/24/microsoft-creates-ai-bot-internet-immediately-turns-racist/. Acesso em: 18 out. 2024.

VENTURA, Felipe. Tecnoblog. **Google fará teste público de tecnologia que imita humano ao telefone.** 2018. Disponível em: https://tecnoblog.net/noticias/2018/06/27/google-duplex-humano-telefone-teste-publico/. Acesso em 18 set. 2024.
YOUTUBE. Google Duplex: **A.I. Assistant Call Local Business to make appointments**. 2018. Disponível em: https://www.youtube.com/watch?v=D5VN56jQMWM. Acesso em 14 out. 2024.

ZUBOFF, Shoshana. **The Age of Surveillance Capitalism**: The Fight for a Human Future at the New Frontier of Power. New York: PublicAffairs, 2019.

7 Information Society and Law
FMU CENTRO UNIVERSITÁRIO

A INTELIGÊNCIA ARTIFICIAL COMO INSTRUMENTO NO COMBATE AOS CRIMES DIGITAIS NA ÁREA MÉDICA

ARTIFICIAL INTELLIGENCE AS A TOOL TO COMBAT DIGITAL CRIME IN THE MEDICAL FIELD

Rodrigo de Carvalho Gonçalves Júnior

Resumo: O artigo procura expor as mudanças na área médica em decorrência das novas tecnologias e os principais meios usados pelos criminosos para obter dados confidenciais dos pacientes. O texto apresenta, inicialmente, o contexto atual da medicina e novas tecnologias, bem como as modalidades de ataques hackers utilizados pelos criminosos na obtenção de dados e como estes conseguem obter vantagem financeira. Posteriormente, aponta alguns casos recentes acerca dos crimes digitais na área médica, a legislação brasileira a respeito da relação médico-paciente e sua aplicação. Ao final traz algumas ideias de como evitar falhas na proteção de dados.
Palavras-Chave: Área médica; novas tecnologias; *hackers*; proteção de dados.

Abstract: This article aims to explain the changes in the medical field due to new Technologies and the main means used by criminals to obtain confidential patient data. The next initially presents the current context of medicine and the Technologies, as well as the types of hacker attacks used by criminals to obtain data and how they can obtain financial advantages. It then points out some recent cases of digital crimes in the medical field, brazilian legislation regarding the doctor-patient relationship and its application. Finally, it provides some ideas on how to avoid data protection failures.
Keywords: Medical field; new Technologies; hackers; data protection.

INTRODUÇÃO

As novas tecnologias têm alterado profundamente as relações interpessoais. Através das inovações técnicas, é possível comunicar-se com pessoas de todo o mundo. Realizar reuniões virtuais, ler um livro digital, interagir com pessoas através de redes sociais são apenas alguns exemplos de como o mundo contemporâneo é altamente tecnológico.

Tal influência é presente na medicina, c com o passar dos anos vêm mudando a relação entre médico e paciente. Com o avanço da tecnologia e da Inteligência Artificial, os serviços médicos tornaram-se mais acessíveis. Atualmente é possível agendar consultas e receber exames através do autoatendimento na web, realizar consultas remotas -facilitando o acesso

dos médicos aos pacientes, realizar o monitoramento contínuo de pacientes com condições médicas fatais informando o médico quando ocorre uma mudança crítica, elaborar prontuários médicos precisos e atualizados e armazenar dados dos pacientes de forma digital.

Os serviços apresentados simplificam a rotina dos pacientes, melhorando o atendimento e influenciando de forma significativa os resultados de pacientes críticos e índices de sobrevivência.

Apesar de muitos benefícios, esse nível de inovação tecnológica expõe hospitais, laboratórios, clínicas médicas e planos de saúde a uma ampla variedade de ameaças de segurança cibernética.

O grande volume de dados de alto valor dos pacientes que as organizações de saúde precisam para manter o padrão de atendimento é alvo de grandes organizações criminosas.

O sequestro de dados dos pacientes atrai os *hackers* devido aos danos imediatos causados. Os criminosos utilizam a mesma lógica dos crimes mais tradicionais: resgate milionário e pouco tempo para negociação.

Na maioria o dos casos, o pagamento de resgate costuma ser exigido por criptomoedas, o que impede o rastreamento do criminoso.

1 CIBER ATAQUE

Os crimes digitais apresentam uma variável muito ampla, desde pequenos roubos a atos de guerra.

Os criminosos usam uma variedade de técnicas para alcançar o objetivo desejado. Na maioria das vezes essa motivação para o crime é totalmente visando um ganho financeiro.

Infelizmente, as instituições de saúde é um grande alvo dos criminosos. Hospitais, clínicas e laboratórios armazenam uma grande quantidade de dados pessoais de pacientes.

Os *hackers* acessam os sistemas com o objetivo de captar esses dados pessoais para cometer o sequestro de identidade, vende-los na *dark* web ou mantê-los como resgate.

Os agentes desta ação criminosa resumem-se a organizações criminosas, atores estaduais e pessoas privadas, sendo divididas em agentes externos e internos.

Os agentes externos são os não autorizados a usar uma rede ou dispositivo, mas entram de qualquer maneira. Correspondem aos grupos criminosos organizados, *hackers* profissionais e amadores.

Os agentes internos são usuários que têm acesso autorizado e legitimo aos ativos de uma empresa. Correspondem aos funcionários, parceiros de negócios, clientes, prestadores de serviços e fornecedores com acesso ao sistema e que usam indevidamente ou acidentalmente seus privilégios.

Os interesses do criminoso em um meio digital visam o dinheiro que é obtido através da coleta de dados do cliente - informações pessoais identificáveis ou outros dados confidenciais.

No âmbito de crimes cibernéticos na área da saúde destacam-se duas espécies: *ransomware* e engenharia social.

2 RANSOMWARE

De acordo com o *X-Force Threat Intelligence Index* da IBM, o *ransomware* é o segundo tipo mais comum de ataque cibernético, representando 17% dos ataques.

Neste caso, os criminosos utilizam um tipo de programa de computador para sequestrar informações pessoais de clientes.

Através deste sequestro, os criminosos exigem um pagamento elevado em troca de não utilizar os dados coletados.

Geralmente, o pagamento do resgate costuma ser exigido em criptomoedas por ser um meio que impede o seu rastreamento.

3 ENGENHARIA SOCIAL

Os crimes de engenharia social é um dos mais espalhados e conhecidos.

Chamado de *phising*, os criminosos compartilham links de divulgação de sites falsos muitos semelhantes aos originais com a emissão de segunda via de boletos.

As mensagens são projetadas para parecer que vêm de uma fonte legitima, mas, ao entrarem nos links, os usuários têm seus dados pessoais e bancários capturados pelos criminosos.

Esse tipo de ação é comum entre os usuários de planos de saúde, pois recebem muitos e-mails e mensagens do plano sobre cobranças e informações.

4 CASOS RECENTES

Em decorrência das novas tecnologias, hospitais, centro de exames, empresas de convênios e órgãos do governo estão cada vez mais dependentes de sistemas digitais.

A tecnologia investida na medicina revolucionou a relação médico-paciente. A Inteligência Artificial transformou mundialmente a área da saúde.

Os aparelhos investidos pelas entidades de saúde vão muito além da assistência médica para elaborar diagnósticos e prevenir doenças. Atualmente, diversas entidades médicas utilizam robôs para armazenar dados de pacientes, agilizar tarefas administrativas e até mesmo serviços de enfermagem.

Esses serviços apresentam maior individualidade, garantindo ao paciente um tratamento mais específico, certeiro e agilizado.

No entanto, os sistemas que armazenam as informações dos pacientes atraem *hackers,* devido à alta quantidade de informações pessoais.

O setor da saúde pública e privada é um grande alvo de ataques cibernéticos.

Segundo pesquisas, 35% dos ataques cibernéticos acontecem contra entidades de saúde. Infelizmente, o Brasil lidera o *ranking* como o país que mais sofre esse tipo de ataque.

Nos últimos anos destacam-se dois ataques sofridos em solo nacional: apagão nas plataformas do Ministério da Saúde e ataque na Unidade de Pronto Atendimento (UPAs) de Presidente Prudente-SP.

O primeiro caso ocorreu em dezembro de 2021, quando um ataque hacker acessou o aplicativo e-SUS Notifica, o Sistema de Informação do Programa Nacional de Imunizações e o “CONCECTE SUS”.

O serviço do SUS ficou fora do ar, o que manchou os levantamentos estatísticos e impossibilitou a emissão de documentos como o Certificado Nacional de Vacinação da COVID-19 e a Carteira Nacional de Vacinação Digital.

O segundo caso é mais recente. Em maio de 2023 uma Unidade de Pronto Atendimento (UPAs) em Presidente Prudente-SP sofreu ataques cibernéticos por três dias. Os ataques afetaram o acesso dos médicos aos prontuários e históricos dos pacientes, sendo necessário realizar todo o trabalho de forma manual, resultando na lentidão das consultas.

Esses ataques acarretam diversas consequências.

As interrupções no sistema de saúde acarretam o atraso de atendimentos,

impossibilitando a equipe médica de realizar exames e acessar os prontuários eletrônicos.

O não acesso ao prontuário eletrônico limitam as informações do paciente quanto ao seu quadro de saúde e histórico, dificultando a tomada de decisão dos médicos.

Além disso, hospitais e empresas de saúde ficam muito prejudicadas financeiramente, pois precisam arcar com multas e indenizações devido ao vazamento de dados dos pacientes, cujo dados pessoais foram vazados.

Em 2021, o hospital *Saint Margareth's Health* nos Estados Unidos foi fechado devido a uma série de ataques cibernéticos. De acordo com o relatório da *American Hospital Association,* mais de 130 hospitais rurais foram fechados desde 2010 nos Estados Unidos. Os ataques cibernéticos atingiram hospitais de diversos tamanhos, mas, especialistas dizem que alguns grupos criminosos se concentram em hospitais e sistemas menores por não possuírem um sistema de defesa adequado. Tal exemplo demonstra a gravidade do impacto financeiro e social causado por um ataque cibernético.

5 A LEI Nº 13.709/2018 (LGPD) NO DIREITO MÉDICO

O direito ao sigilo, à privacidade, à autonomia e à dignidade são garantias previstas na Constituição Federal de 1988, e, a Lei n°13.709 de 14 de agosto de 2018(LGPD) veio como um instrumento do Estado para reforçar a proteção desses direitos constitucionais.

Quando se trata de saúde, essa proteção torna-se ainda mais importante, pois os sistemas dos hospitais, clínicas, laboratórios e empresas de convênio médico são ricas em informações intimas do paciente, que são imprescindíveis para o exercício da medicina.

A coleta de dados do paciente é imprescindível para o exercício da atividade. O histórico de saúde e as condutas do profissional são registradas por meio do prontuário, um documento que reúne informações do paciente, sinais e imagens registradas de exames, acontecimentos e situações sobre a saúde do paciente e a assistência a ele prestada, conforme definido pelo Conselho Federal de Medicina, Resolução CFM n°1.638/2002.

6 A IMPORTÂNCIA DOS DADOS NA RELAÇÃO MÉDICO-PACIENTE

De acordo com os dados fornecidos, o médico elabora a anamnese, um procedimento essencial para que a equipe de saúde possa compreender o histórico e os sintomas do paciente para chegar a um diagnóstico.

Para a elaboração deste relatório é essencial que exista uma relação de confiança entre paciente e o profissional da saúde. Quanto maior a riqueza de detalhes coletados maior será a eficácia do tratamento médico.

7 PROTEÇÃO NORMATIVA DOS PACIENTES

Com a LGPD em vigor, o cuidado médico referente às informações dos pacientes teve que ser redobrado devido às sanções administrativas descritas na lei.

Como mencionado anteriormente, a LGPD veio para reforçar a proteção de direitos previstos na Carta Magna e outras leis.

Podemos encontrar a garantia da proteção de dados nas seguintes normas e resoluções:

Constituição Federal de 1988: é constitucional o direito a dignidade da pessoa humana, intimidade, vida privada, honra e imagens. É assegurado o direito de indenização pelo dano material ou moral decorrente de sua violação.

Código Civil: de acordo com a legislação civil, os direitos da personalidade são irrenunciáveis. É possível ao titular exigir que cesse a ameaça, ou a lesão, e reclamar perdas e danos.

Código Penal: a legislação penal tipifica o crime de violação de segredo profissional. Artigo 154, Código Penal: “revelar alguém, sem justa causa, segredo, de que tem ciência em razão de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem: Pena-detenção, de três meses a um ano, ou multa”.

Código de Ética Médica: elenca os deveres de sigilo e respeito à autonomia do paciente.

Resolução CFM n°1605/00: garante ao paciente que o conteúdo do seu prontuário ou ficha médica não será revelado sem seu consentimento.

Resoluções CFM n°1.821/07 c 2.218/18:aprova as normas técnicas concernentes à digitalização e uso dos prontuários dos pacientes, autorizando a eliminação do papel c a troca de informação identificada cm saúde.

As resoluções são hierarquicamente inferiores às leis. Havendo incompatibilidade entre uma resolução do Conselho Federal de Medicina e a Lei Geral de Proteção de Dados (LGPD), prevalecerá a regra da lei.

8 RESPONSABILIDADE DOS MÉDICOS, CLÍNICAS E HOSPITAIS

Quando ocorre uma invasão bem-sucedida ao sistema de saúde ou membros da equipe médica compartilham dados pessoais de pacientes, a LGPD elenca sanções administrativas a serem aplicadas pela Autoridade Nacional de Proteção de Dados (ANPD).

As sanções administrativas (multas) não excluem as responsabilidades cíveis e penais resultantes da falha de segurança de dados.

9 COMO EVITAR FALHAS NA PROTEÇÃO DE DADOS?

A Lei Geral de Proteção de Dados determina que sejam utilizadas medidas técnicas e administrativas para proteger os dados pessoais de acessos não autorizados e de situações acidentais, ilícitas e de situações de destruição, perda, alteração, comunicação e difusão de dados.

Com a crescente evolução das tecnologias e suas inovações, a medicina passa por um processo de modernização constante, trazendo muitos benefícios para os profissionais da saúde e pacientes. No entanto, o mundo do crime evoluiu e trouxe várias vulnerabilidades aos sistemas operacionais das instituições de saúde.

Ao mesmo tempo que houve melhorar significativas na área da saúde houve vulnerabilidades nos sistemas que permitiram o acesso de hackers nos sistemas, causando prejuízos milionários.

Segundo cálculos da International Business Machines (IBM), a violação de dados na área da saúde trouxe um prejuízo de 10 milhões de dólares, somente em território americano, e os custos decorrentes desses ataques cresceram 42% desde 2020.

Para evitar esses prejuízos milionários, é preciso adotar medidas rápidas na área de saúde. Instituições públicas e privadas precisam investir em cibersegurança para garantir maior proteção dos dados. Investir na segurança dos dados para bloquear acessos indevidos é necessário, mas, só isso não basta.

A adoção de medidas tecnológicas não é suficiente para a proteção jurídica dos agentes de tratamento de dados, pois a maioria das falhas na segurança resulta de ação humana.

Por isso, é necessário realizar um treinamento e conscientização de todos aqueles que trabalham na unidade e que possam ter acesso aos dados dos pacientes.

A LGPD destaca a importância da adoção de práticas de governança e políticas

internas que demonstrem o compromisso com a segurança dos dados.

CONCLUSÃO

Devido às novas tecnologias usadas na medicina, a relação médico-paciente foi profundamente alterada.

A Inteligência Artificial tornou-se uma grande aliada da área da saúde, sendo responsável por armazenar dados dos pacientes, apresentar diagnósticos, monitorar pacientes e realizar atuação preventiva. No entanto, as instituições públicas e privadas de saúde são um grande alvo para os criminosos devido ao grande armazenamento de dados confidenciais de pacientes.

A motivação financeira é o principal objetivo para a realização de sequestro de dados. As informações obtidas podem ser muito lucrativas para os criminosos, c este tipo de crime está cada vez mais frequente.

Hospitais, laboratórios, clínicas e empresas de convênio estão cada vez mais dependentes dos sistemas digitais, devido aos benefícios gerados, como celeridade e assertividade. Mas, infelizmente tais sistemas estão cada vez mais expostos a sofrerem ataques cibernéticos devido a falha técnicas e falhas humanas.

Um ataque cibernético bem-sucedido pode gerar graves prejuízos aos pacientes, aos profissionais da saúde e instituições.

Para assegurar os direitos destes pacientes e profissionais, a Lei n° 13.709/2018(LGPD) tem um papel muito importante.

A Lei Geral de Proteção de Dados (LGPD) tem por objetivo reforçar direitos constitucionais relacionados à privacidade e intimidade, assim como regulamentar as condutas médicas no meio digital, garantindo maior segurança aos médicos, pacientes e sistemas operacionais.

REFERÊNCIAS

BRASIL. **Constituição da República Federativa do Brasil**. 5 de outubro de 1988.

BRASIL. **Lei n° 10.406,10 de janeiro de 2002.** Código Civil.

BRASIL. **Decreto-Lei n° 2.848, 7 de dezembro de 1940.** Código Penal.

BRASIL. **Lei n°13.709, 14 de agosto de 2018**. Lei Geral de Proteção de Dados.

CONSELHO FEDERAL DE MEDICINA (CFM-BRASIL). **Resolução n°1.605, 15 de setembro de 2000.**

CONSELHO FEDERAL DE MEDICINA (CFM - BRASIL). **Resolução n°1.821, 11 de julho de 2007.**

CONSELHO FEDERAL DE MEDICINA (CFM-BRASIL). **Resolução n°2.218, 21 de setembro de 2018.**

CONSELHO FEDERAL DE MEDICINA (CFM-BRASIL). **Resolução n°1.638, 10 de julho de 2002.**

BONFIM, BRUNA. **Ataques cibernéticos prejudicam atendimentos nas UPAs de Presidente Prudente.** Veja, 2023. Disponível em: https://g1.globo.com/sp/presidente-prudente-regiao/noticia/2023/05/27/ataques-ciberneticos-prejudicam-atendimentos-em-upas-de-presidente-prudente.ghtml Acesso em 22 de outubro de 2024.

FELIX, PAULA. **Setor de saúde tem epidemia de hackers** – e Brasil é um dos mais expostos. Veja, 2024. Disponível em: https://veja.abril.com.br/saude/setor-de-saude-tem-epidemia-de-hackers-e-brasil-e-um-dos-mais-expostos#googlevignette Acesso em 22 de outubro de 2024.

NETO, Miguel; NOGAROLI, Rafaella. **Debates Contemporâneos em Direito Médico e da Saúde**-Ed. 2023. São Paulo (SP): Editora Revista dos Tribunais.

SOUTHWICK,RON. **After cyberattack and other financial woes, an Illinois hospital closes its doors.** Chief healtcare executive, 2023. Disponível em: https://www.chiefhealthcareexecutive.com/view/after-cyberattack-and-other-financial-woes-an-illinois-hospital-closes-its-doors Acesso em 22 de outubro de 2024.

QUINTINO DE OLIVEIRA JÚNIOR, Eudes. FRANCIELE NEVES DE OLIVEIRA, JÚLIA. **Lei geral de proteção de dados e o tratamento de dados na saúde.** Migalhas, 2023. Disponível em: https://www.migalhas.com.br/coluna/leitura-legal/385614/lei-geral-de-protecao-de-dados-e-o-tratamento-de-dados-na-saude Acesso em 22 de outubro de 2024.

TECNOLOGIA DA INFORMAÇÃO. **Informativo SPDM. Ciberataques na área da saúde.** Disponível em: https://spdm.org.br/wp-content/uploads/2022/06/2a-Ed.-CIBERATAQUES-NA-AREA-DE-SAUDE_Rev.pdf Acesso em 22 de outubro de 2024.

O QUE É UM ATAQUE CIBERNÉTICO. IBM. Disponível em: https://www.ibm.com/br-pt/topics/cyber-attack Acesso em 22 de outubro de 2024.

7 Information Society and Law
FMU CENTRO UNIVERSITÁRIO

PROVA PERICIAL, CADEIA DE CUSTÓDIA E EVIDÊNCIAS DIGITAIS: DESAFIOS NA ERA DA INFORMAÇÃO

EXPERT EVIDENCE, CHAIN OF CUSTODY, AND DIGITAL EVIDENCE: CHALLENGES IN THE INFORMATION AGE

André Luiz Viana Borges[1]; Cassia Luize Ferreira da Silva [2]; Irineu Francisco Barreto Junior[3]

Resumo: Este artigo explora a importância da prova pericial e da proteção do processo de produção e tratamento de provas através da Cadeia de Custódia. A cadeia de custódia é discutida como um conjunto de procedimentos essenciais que garantem a integridade e admissibilidade das evidências ao longo de sua coleta, armazenamento e análise durante investigações criminais e processos judiciais. A legislação recente, a partir de 2019, que detalhou os procedimentos da cadeia de custódia no Brasil e tornou seu uso obrigatório no contexto judicial, é destacada. O estudo também aborda os desafios específicos enfrentados na coleta, preservação e análise de evidências digitais, cada vez mais presentes nas investigações. A natureza variável das evidências digitais demanda técnicas especializadas e atualizadas para sua interpretação correta e uso como prova válida. Em resumo, este trabalho analisa a questão da prova pericial e da cadeia de custódia normatizada pelo "Pacote Anticrime" diante do avanço das tecnologias digitais, sublinhando a importância da conformidade com normas legais e técnicas para garantir a integridade e validade das evidências digitais nos processos judiciais.
Palavras-Chave: Prova Pericial; Cadeia de Custódia; Sociedade da informação; Evidência digital

Abstract: This article explores the importance of expert evidence and the protection of the process of producing and handling evidence through the Chain of Custody. The chain of custody is discussed as a set of essential procedures that ensure the integrity and admissibility of evidence throughout its collection, storage, and analysis during criminal investigations and judicial proceedings. Recent legislation, since 2019, which detailed the procedures of the chain of custody in Brazil and made its use mandatory in the judicial context, is highlighted. The study also addresses specific challenges faced in the collection, preservation, and analysis of digital evidence, which are increasingly present in investigations. The variable nature of digital

[1] Perito Criminal, bacharel em direito, físico, mestrando em Direito da Sociedade da Informação nas Faculdades Metropolitanas Unidas.
[2] Advogada, mestranda em Direito da Sociedade da Informação nas Faculdades Metropolitanas Unidas.
[3] Pós Doutor em Sociologia pela Faculdade de Filosofia, Letras e Ciências Humanas da Universidade de São Paulo – USP-SP. Doutor em Ciências Sociais pela Pontifícia Universidade Católica de São Paulo – PUC-SP. Professor do Programa de Mestrado em Direito da Sociedade da Informação e do Curso de Graduação em Direito da FMU-SP. Coordenador do Grupo de Pesquisa CNPQ Ética e Fundamentos Jurídico-Políticos na Sociedade da Informação. Analista de Pesquisas da Fundação Seade –São Paulo. Pesquisador FAPESP do Centro de Ciência de Dados para Estatísticas Públicas.

evidence requires specialized and up-to-date techniques for its correct interpretation and use as valid evidence. In summary, this work analyzes the issue of expert evidence and the chain of custody standardized by the "Anti-Crime Package" considering advances in digital technologies, emphasizing the importance of compliance with legal and technical standards to ensure the integrity and validity of digital evidence in judicial proceedings.
Keywords: Expert Evidence; Chain of Custody; Information Society; Digital Evidence.

INTRODUÇÃO

O desenvolvimento vertiginoso das tecnologias de informação e comunicação trouxe consigo uma proliferação de evidências digitais, que são frequentemente cruciais na resolução de processos judiciais. Entretanto, a forma como essas provas são coletadas, preservadas e apresentadas pode impactar significativamente a investigação e o resultado do processo, particularmente no âmbito penal.

Este artigo visa explorar esses desafios específicos relacionados com a prova pericial, a cadeia de custódia e as evidências digitais, examinando a evolução legislativa relacionada com a prova pericial e a implementação da cadeia de custódia no Brasil, especialmente após a promulgação da Lei nº 13.964 de 24 de dezembro de 2019, conhecida como "Pacote Anticrime". A rápida evolução tecnológica e a crescente digitalização das atividades humanas geram tipos de evidências que são substancialmente diferentes das provas físicas tradicionais.

As evidências digitais podem assumir inúmeras formas, incluindo registros de comunicações eletrônicas (e-mails, mensagens instantâneas), dados de localização geográfica, informações armazenadas em nuvem, logs de sistemas, vídeos e imagens digitais, entre outras. Cada tipo de evidência digital apresenta características específicas que modificam a forma de sua coleta e preservação. Ademais, dados digitais podem ser facilmente alterados, deletados ou corrompidos, muitas vezes sem deixar rastros perceptíveis.

No processo penal, a confiabilidade e a integridade das provas são fundamentais para assegurar decisões justas. Falhas na preservação da cadeia de custódia ou na autenticação das provas podem resultar na inadmissibilidade das evidências, comprometendo seriamente o resultado do processo.

Assim, a produção de provas periciais no direito penal enfrenta inúmeros desafios na era da informação, desde a manipulação dos dados digitais até a autenticação das informações provenientes de diversas fontes tecnológicas. As provas digitais, pela sua natureza volátil e facilmente alterável, requerem técnicas avançadas de coleta e preservação para garantir sua

integridade. Esse cenário exige um nível elevado de expertise técnica e um robusto arcabouço normativo para orientar as práticas forenses.

A cadeia de custódia é um conceito central na prática forense e que se tornou ainda mais rigorosa com a promulgação do "Pacote Anticrime". Essa legislação introduziu diretrizes claras para a manutenção da integridade das provas, normatizando procedimentos detalhados, que asseguram a integridade e a imparcialidade dos indícios coletados e que devem ser seguidos pelos profissionais responsáveis pela coleta e análise de evidências.

A inclusão formal do conceito de cadeia de custódia no arcabouço legal brasileiro é um avanço significativo que busca padronizar os procedimentos de manuseio de provas, minimizando o risco de contaminação ou perda de evidências, de forma a garantir a confiabilidade das provas apresentadas em juízo, assegurando, como fim último, o devido processo legal.

Não obstante, embora a normatização desse conceito represente um avanço significativo, a legislação não previu de forma específica os procedimentos relacionados com a coleta, preservação e apresentação de evidências digitais. A ausência de uma regulamentação específica para as evidências digitais deixa lacunas que podem gerar controvérsias durante os processos judiciais. Dado o caráter mutável e volátil das provas digitais, é imperativo que o arcabouço legal evolua continuamente para acompanhar as inovações tecnológicas e as novas formas de criminalidade.

Outro desafio significativo é a infraestrutura tecnológica necessária para a implementação eficaz das novas diretrizes. Equipamentos adequados para a coleta, armazenamento e análise de evidências digitais são essenciais para garantir que essas provas sejam mantidas intactas e seguras. Além disso, a criação de bancos de dados seguros, sistemas de rastreamento de provas e a implementação de protocolos padronizados demandam investimentos substanciais. Sem esses recursos, a cadeia de custódia pode ser comprometida, colocando em risco a validade das evidências apresentadas em juízo.

Assim, o objetivo deste artigo é discutir de forma abrangente a produção e o tratamento de provas periciais, incluindo as evidências digitais, no contexto do direito penal, analisando o impacto do recente conceito de cadeia de custódia introduzido pelo "Pacote Anticrime". A importância de garantir a integridade das provas e a justa aplicação da lei emerge como a

justificativa principal para este estudo, que se alinha com os princípios fundamentais do devido processo legal.

Pretende-se responder o seguinte problema de pesquisa: Quais são os principais desafios relacionados com as evidências digitais e como esses desafios influenciam a integridade e admissibilidade das provas no sistema judiciário brasileiro após a introdução do "Pacote Anticrime"?

Para abordar essa questão, foi feita uma pesquisa exploratória aliada ao método dedutivo reflexivo-crítico, por meio de uma ampla pesquisa bibliográfica, na qual consultaram-se artigos, teses e legislação.

O artigo foi dividido em três seções, quais sejam: 1) Prova pericial; 2) Cadeia de custódia; e 3) Evidências digitais.

1. PROVA PERICIAL

No campo das Ciências Forenses, a interdisciplinaridade é fortemente presente. Áreas do conhecimento humano, tais como Biologia, Física, Química, Medicina, Tecnologia, dentre outras, exercidas por Peritos Criminais e Médicos Legistas, aliam-se ao Direito, à Criminologia e à Criminalística para auxiliar e orientar as partes componentes do sistema Judiciário para que a Justiça seja aplicada de modo parcimonioso e escorreito.

A atividade jurídica é exercida por humanos que são inerentemente influenciáveis e conduzidos, frequentemente, por ímpetos decisórios em que pesam – muitas vezes inconscientemente, portanto, são ausentes elementos de intencionalidade – vieses cognitivos, dentre eles, a “Ilusão do Controle”.

O magistrado brasileiro, quando “dizendo o Direito” – sua atividade primária – deve ter alguns princípios em mente: entre eles a presunção da não culpabilidade e, principalmente, o devido processo legal. Deve também ter o cuidado de sopesar todas as informações que lhe são fornecidas (provas periciais, depoimentos e inclusive suas convicções pessoais) quando tomando suas decisões. Apesar da aparente liberdade que lhe daria o princípio do livre convencimento, vale lembrar que este deve ser devidamente motivado, como propõe Dworkin:

> O ato de decidir não pode ser visto como a possibilidade de os julgadores escreverem uma série de contos independentes, sem qualquer correlação entre si, mas, ao contrário, antes, devem ter o compromisso com um romance único, cujo enredo se mostre integrado. (Dworkin, 2007, p. 275 apud Iribure Júnior; Rosa, 2018, p. 46).

1.1 Breve histórico da perícia no mundo

É possível encontrar diversas pesquisas cujos autores mencionam evidências de que a "perícia" técnica já era uma demanda em civilizações tão longínquas quando os egípcios e hebreus. Entretanto, segundo Santos (1908, apud SILVA, 2010), foi a partir dos Romanos, com suas Leis das XII Tábuas, que passou a existir uma indicação mais clara da utilização da perícia como meio de prova transcendendo o desenvolvimento das diversas períodos de seu sistema processual.

Silva (2010) menciona que o processo civil romano tem três grandes períodos: o das ações da lei (legis actiones), o formulário (per formulas) e o extraordinário (cognitio extraordinaria).

Ainda segundo Silva:

> O processo era dividido inicialmente em duas fases nos dois primeiros períodos: in iure (fase que se dá diante do magistrado, do pretor, que apreciava a ação sob o aspecto jurídico e legal) e apud iudicem ou in iudicio (fase que se processa perante o iudex, particular, não representante do Estado, que julga a causa) (2010, p. 18).

De acordo com Santos (1908, apud SILVA, 2010), o momento de produção de provas era o in iudicio, atuando o próprio iudex como órgão verificador quando se tratava de exame ou inspeção visual (ocular). Esse era o exame judicial. O litígio era dado a conhecer ao iudex e julgava de maneira soberana – em nome do povo – não se subordinando hierarquicamente a nenhum outro órgão.

Tal exame, vistoria, ou inspeção visual, assim em Roma como em outros lugares, começou como um ato exclusivo e pessoal do juiz, que originalmente certificava-se, pessoalmente, sobre a materialidade dos fatos e dos vestígios do acontecido, como indica Silva (Silva, 2010).

Já durante o terceiro período, o extraordinário, suprimiram-se as duas fases processuais, passando a instância inteiramente ao magistrado, servidor do Estado. Mudança ocorrida em 294 (D.C.), com a Constituição de Diocleciano, que generalizou a cognitio extraordinaria, concentrando as funções de declarar o direito e julgar os fatos na pessoa do magistrado. Era diante deste que se desenvolvia toda a relação processual, desde o início, com a petição inicial, até seu término, com a execução.

Nesse momento, o juiz – que não é mais indicado pelas partes, mas sim um funcionário do Estado – nem sempre conta com todos os conhecimentos técnicos necessários para atender

e julgar todos os tipos de litígios que lhe são submetidos, aumentando a necessidade de acudir à figura do perito, a quem o juiz – dadas suas limitações de conhecimento técnico – delega a função de decidir sobre assuntos mais técnicos, como revelam amplamente as fontes.

De fato, segundo Santos (1908, apud SILVA, 2010), existia, nas leis romanas, a previsão legal da atuação do perito em casos de gravidez de mulher divorciada, quando o juiz poderia ordenar o exame por três parteiras e também em casos de restabelecimento de marcos apagados por enchentes em lindes imobiliárias, quando se recorria aos agrimensores, havendo apenas a observação de que, para alguns doutrinadores, aqueles apenas funcionariam como árbitros, e não propriamente como peritos, mencionando também as avaliações de plantações, bens que eram submetidos à Administração Pública.

Há diversos exemplos sobre a intervenção dos peritos, com destaque ao caso descrito na tábua de Málaga, capítulos 64 e 65, que defere a homens entendidos a avaliação de imóveis oferecidos em garantia pelos devedores do fisco.

Há que se mencionar também o desenvolvimento da prova literal, que mostra a evolução da perícia em documentos, que era feita com relação a sua autenticidade, e poderia ser realizada tanto em casos de comparação de escrita como quando arguida a falsidade documental.

Segue-se a queda do Império Romano e a consequente desagregação social que imperou por certo tempo no continente europeu, com grande influência da Igreja Católica Apostólica Romana, que como herdeira "natural" de Roma, exerceu, ao mesmo tempo, o poder temporal e espiritual em grande parte da civilização espiritual, durante séculos. Nesse sentido, há que se mencionar que a perícia teve um bom impulso e sobreviveu graças ao Direito Canônico, em que o sistema de provas progrediu graças à cultura dos membros do clero e à necessidade de substituir o sistema das ordálias, que a Igreja condenava devido à sua barbárie. Assim, a prova obtida por inspeção ocular de pessoas e coisas, tanto realizada por juiz como por peritos, voltou a ganhar importância, assumindo diversas formas.

O exame judicial passou, dessarte, a ser utilizado no estabelecimento das linhas divisórias de imóveis, nos embargos de obra nova e constatação de fatos, e, no que se refere a pessoas, em causas ligadas a suas idades. Já o exame pericial foi usado nas causas ligadas ao divórcio por impotência e quanto à prova de virgindade.

Com esse impulso dado pelo Direito Canônico, a perícia passou a ser admitida por vários povos no final da Idade Média, graças também ao estudo do Direito Romano, e à influência de ambos sobre a sistematização das provas judiciárias, embora estas ainda fossem confundidas com o exame judicial e o juízo arbitral.

Apesar disso, a perícia já se encontrava, no Início da Idade Moderna, entre os meios de prova, inclusive com a separação do exame judicial do pericial, visto ser impossível exigir-se dos juízes um conhecimento universal. A legislação passou, a partir daí, o encargo do exame de pessoas ou coisas para indivíduos versados nas artes ou nas ciências.

Em tempos mais modernos – nos diz Silva (2010) –, com a evolução das artes e das ciências ocorridas durante o Renascimento, e com o consequente resgate de áreas do conhecimento e valores da antiguidade greco-romana, além do desenvolvimento do que viria a ser chamado de método científico, as ordenanças jurídicas europeias já traziam a perícia com as características básicas atuais, tal como podia ser visto, por exemplo, na Ordenança de Blois, na França, que em 1579 trazia expressamente que o valor das coisas seria decididos por peritos, não por testemunhas. Isso teve uma repercussão tal que foi instituída uma corporação de peritos para servirem como auxiliares dos juízes em questões técnicas.

Em 1667, acabou-se por retomar a tradição romana de conceder às partes o direito de escolher o perito, após serem reconhecidos problemas dentre a escolha obrigatória entre apenas algumas pessoas de uma corporação. Houve também excessos na prática de perícias nessa época, sendo necessário, por exemplo, que o Parlamento Francês suprimisse, em 1677, a perícia de cópula carnal em caso de nulidade de casamento, prática que fora "copiada" dos tribunais eclesiásticos.

Diferentemente da França, a Inglaterra adotou, pelos costumes, a inspeção judicial. Já na Itália foram utilizadas tanto a perícia como o exame judicial e o juízo arbitral.

No início do século XIX, o Código Civil francês de 1804, seguido pelo CPC de 1806, foi baseado na ordenança de 1667 e inspirou-se em princípios revolucionários, entre os quais a liberdade de trabalho.

A Assembleia Constituinte deu tamanha importância à liberdade de trabalho que acabou suprimindo o privilégio profissional dos peritos oficiais, permitindo que os peritos fossem escolhidos livremente em qualquer classe social, inclusive entre aqueles cuja profissão

não fosse a do objeto de litígio, desde que tivessem competência especial sobre a matéria que deveria ser tecnicamente apreciada.

O Brasil Colonial foi regido por duas Ordenações – como eram chamados os códigos legais no mundo português – as Manuelinas e as Filipinas, sendo que a segunda – a que efetivamente foi usada – vigorou quando a metrópole estava sob jugo espanhol. Esse código tinha institutos mais sistematizados e trazia uma adaptação do direito Romano-Justiniano.

Segundo Silva (2010), nas Ordenações Filipinas, o legislador estabeleceu clara e minuciosamente a forma de escolha dos peritos e os respectivos compromissos e juramentos, prevendo inclusive a possibilidade de escolher um terceiro perito para dirimir eventuais discordâncias, além de estabelecer diretrizes a serem seguidas. Também havia a distinção expressa entre o perito ou arbitrador e os juízes árbitros, algo que não era claro em outras legislações, como nos informa Almeida (1870, apud SILVA, 2010).

Essas ordenações foram conservadas e revalidadas com a restauração da Coroa Portuguesa em 1640, com a subida de João VI ao trono e vigorou parcialmente no Brasil até a entrada em vigor do Código Civil de 1916.

1.2 A perícia no ordenamento jurídico brasileiro

A legislação brasileira sofreu direta influência do Código Francês e das Ordenações Filipinas. Essa influência também se estende à Medicina Legal durante o período colonial, embora esta tenha sofrido – em uma escala menor – também a influência de italianos e alemães. A influência portuguesa foi mínima, segundo Croce e Croce Júnior (2009), resumindo-se quase que totalmente à toxicologia.

De acordo com Lima (2008, apud SILVA, 2010, p. 49), a família real, ao chegar ao Brasil, cria a Escola de Cirurgia da Bahia – a primeira instituição de ensino superior no território – tendo papel preponderante o médico brasileiro e Cirurgião-Mor do Reino, José Correia Picanço, pernambucano de nascença.

Conforme Croce e Croce Junior (2009), em uma segunda fase, iniciou-se o ensino prático da Medicina Legal, pelas mãos de Agostinho José de Souza Lima, desenvolvendo a pesquisa laboratorial, limitada até esse momento à Toxicologia, e realizando interpretações e comentários médico-legais à legislação vigente, mesmo não havendo cursado Direito.

Já sob o Império – após a Independência – o Código Criminal, promulgado em 1832, trouxe conteúdo progressista, inclusive no que se relacionava à perícia. Nele, observava-se que o Juiz de Paz era responsável por determinar os peritos que iriam participar de cada perícia em específico, assinando – junto a eles – o laudo.

Com a alteração sofrida pelo código, em 1841, criaram-se os cargos de Chefe de Polícia, Delegados e Subdelegados, estabelecendo-se, desta forma, a chamada "polícia judiciária", que era responsável pela realização do corpo de delito (PIERANGELI, 1983).

Mudando o enfoque da área criminal para a área cível, vê-se que a perícia era, naquele momento, chamada de arbitramento (CINTRA, GRINOVER, CAMARGO, 2001). Segundo a legislação vigente à época para os processos de natureza civil, o arbitramento seria solicitado pelas partes, que poderiam indicar quem desejariam que arbitrasse sua lide e os peritos escolhidos eram nomeados pelo juiz em audiência específica. Também poderia haver uma nomeação exofficio caso as partes não os indicassem. No processo civil, o arbitramento não restringia o juiz, que podia determinar outro perito caso houvesse divergência entre os três arbitradores.

Essas regras permaneceram válidas durante o período de dualidade processual, entre 1891 e 1934, quando era permitido aos Estados legislar sobre Direito Processual e foram acolhidas pelos códigos estaduais. Posteriormente, mantiveram a forma com o restauro da unicidade (SILVA, 2010).

Após a queda do Império, seguiu-se a evolução do ordenamento jurídico pátrio, com a instituição dos Códigos: Penal (1940), de Processo Penal (1941), Civil (na versão atual de 2002) e de Processo Civil (de 2015).

Com o passar do tempo, houve a construção do conceito de prova pericial – nos diz Oliveira (2019) –, tanto na doutrina como na jurisprudência, coadunando-se com o ordenamento jurídico nacional, tratando, de maneira geral, a questão da prova como essencial para o desenrolar de todo o processo e a tomada de decisões. Para isso, ainda segundo Oliveira, a reforma no Código de Processo Penal em 2008 foi notoriamente importante, pois com a lei n.º 11.690 de 2008, instituíram-se sensíveis modificações quanto ao sistema probatório em geral, e em relação a prova pericial. Hoje, está claro que nos códigos processuais, tanto no Penal como no Civil, o legislador tomou especial cuidado em dedicar seções inteiras aos Peritos e às perícias.

A última alteração substancial ao Código de Processo Penal, a Lei n.º 13.964 de 2019 – popularmente alcunhada como "Pacote Anticrime" – agregou a normatização do Cadeia de Custódia, que apesar de ser uma prática já conhecida e praticada entre os profissionais de perícia atuantes nas instâncias brasileiras, carecia de uma fundamentação jurídica e da consequente normatização, que finalmente veio e passou a vigorar, após o período da vacatio legis, no início de 2020.

Apesar dessa aparente "inovação" na legislação com referência à Cadeia de Custódia, faz-se importante notar – como mencionam Giacomolli e Amaral (2020) – que já havia normatização vigente tratando de procedimentos que devem ser observados quanto à manutenção da cadeia de custódia dos vestígios: por exemplo, a Portaria n.º 82 da Secretaria Nacional de Segurança Pública, de 16 de julho de 2014. Documento que estabelece diretrizes sobre tais procedimentos, trazendo detalhes mais aprofundados para a implementação de uma cadeia de custódia mais eficiente.

Apesar disso, apontam Giacomolli e Amaral, na prática tais documentos – como por exemplo a Portaria n.º 82, da SENASP – não produziu os efeitos que se esperavam. Por essa razão, pode-se considerar que o legislador andou bem na implementação das alterações legislativas, constituindo-se a implementação da Cadeia de Custódia em uma mostra da valorização do instituto da prova – e, de maneira indireta, dos profissionais que com elas lidam –, refletindo um momento que está presente em nível de América Latina. Interessante saber que o modelo seguido é o da legislação colombiana, que em sua codificação processual penal (Colômbia, 2004) também tem um capítulo destinado à regulamentação geral da Cadeia de Custódia.

2 CADEIA DE CUSTÓDIA

A prova pericial, qualquer que seja sua origem, deve ser produzida adequadamente, de modo a ser considerada válida e, assim, subsidiar de maneira substancial e inequívoca as decisões do juiz em sua busca da verdade real – como tradicionalmente preconizava o CPP. Para garantir essa "qualidade" em termos de inviolabilidade, existe a série de procedimentos chamada de Cadeia de Custódia, que, como ensina Espindula (2009), tem como principal finalidade garantir a idoneidade dos objetos e bens recolhidos escolhidos pela perícia ou apreendidos pela autoridade policial – durante a fase investigatória ou mesmo na fase de

persecução penal – evitando qualquer tipo de dúvida quanto à sua origem e ao caminho que percorreu no decurso da investigação criminal e processo judicial correspondente.

Considera-se cadeia de custódia, nesse sentido, "o conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou vítimas de crimes, com a finalidade de rastrear sua posse ou manuseio" (CPP, art. 158-A, 2019) – a partir de seu reconhecimento até seu descarte.

Seu início se dá a partir da preservação do local do crime ou por meio de procedimentos policiais ou periciais com os quais detecte-se a existência de vestígio. De acordo com a doutrina e com a própria legislação (CPP e, subsidiariamente, o Código de Processo Civil, CPC, em seu capítulo II, seção II) a coleta dos vestígios será feita preferencialmente por peritos oficiais – visto que a análise posterior deles quase que certamente dependerá de conhecimentos técnicos e científicos –, que darão o encaminhamento necessário para a central de custódia, mesmo quando necessária a realização de exames complementares (conforme os artigos 158- A a 158-F, do CPC, acrescentados pela lei n.º 13.964 de 2019).

Cabe aqui considerar, entretanto, que a cadeia de custódia é constituída pelas formas que devem ser seguidas no desempenho das tarefas de recolhimento, conservação, manipulação, transporte e entrega no laboratório de destino dos materiais que serão submetidos a exame, bem como todos os procedimentos internos laboratoriais até a emissão do laudo pericial, com o fim de garantir que a substância ou objeto analisado seja o mesmo que o apreendido, produzindo, desse modo, uma prova lícita, efetiva e sem vulneração do estado de direito de defesa dos acusados. Destarte, a cadeia de custódia da prova não é de competência absoluta dos peritos, senão também de todos os envolvidos nas esferas investigativas e processuais (BRÁZ, 2019).

Tal instituto do processo penal tem como uma de suas bases principiológicas o princípio da documentação, assim como o da descrição, da análise, da associação, da reconstrução, da classificação, da individualização, da identificação, e da transferência, e parte do conjunto de princípios da Criminalística, que, geralmente, são profundamente estudados no âmbito pericial e parcamente considerados no ensino jurídico.

O princípio da documentação preconiza que toda amostra deve ser documentada, desde seu nascimento no local de crime, até o momento de sua análise e descrição final, de modo a estabelecer um histórico completo e fiel de sua origem. Demonstra a necessidade de documentar

tudo aquilo que ocorre no "caminho do vestígio", quer dizer, não se pode realizar a coleta de um material sem que haja a documentação, o registro documental do que se está realizando.

Este princípio se coaduna com o princípio da "mesmidade" – descrito pela primeira vez no âmbito da cadeia de custódia por Ruben Darío González (2016) –, que prevê que o elemento analisado e utilizado em juízo seja realmente o recolhido na cena, que a interpretação da análise da evidência reflita exatamente o que ocorreu e, ainda, que o estado do elemento tenha sido conservado em condições idênticas às que se encontrava no local do crime. Assim, documentar o caminho percorrido por um elemento assegurará que, no futuro, o princípio da mesmidade seja rapidamente comprovado. Sem a documentação, a mesmidade é afastada e se esvai no nada.

Deste modo, ao se associarem os princípios da documentação e da mesmidade, construir-se-á uma base epistêmica que fundamenta a cadeia de custódia da prova pericial. O entendimento desses princípios, associados ao estudo da criminalística, é de importância cabal para o entendimento da prova científica.

Cabe lembrar que a simples apresentação da prova pericial à justiça não garante, por si só, sua aceitabilidade ou validade jurídica. Esta será garantida por meio da Cadeia de Custódia, ou seja, a documentação, por parte do órgão de análise, contendo o rastreio de todas as operações realizadas com cada um dos vestígios, desde sua coleta no local do fato criminosa, até sua completa destruição. Tal processo começa muito antes da ação penal: geralmente, a autoridade policial e seus agentes, ao se dirigirem ao local dos fatos para apurarem as circunstâncias, têm, portanto, o primeiro contato com a prova em si, sendo sua maior responsabilidade – conforme o artigo 6º, I, do CPP – garantir que não sejam alterados o estado e a conservação das coisas até que cheguem os peritos, que executarão a parte técnica da prova.

Caso haja alterações no local do crime, o artigo 169, parágrafo único, do CPP preconiza que os peritos deverão proceder ao registro em seu laudo de eventuais alterações e como elas impactam os exames efetuados e, em especial, suas conclusões.

Importante aqui faz-se mencionar que, pese a toda a importância desse cuidado procedimental, não havia, até 2019, uma normatização efetiva sobre o procedimento da Cadeia de Custódia, situando-se esta no âmbito das "boas práticas" em perícia. As ideias gerais, observam Magno e Comploier (2021), estavam previstos no Código de Processo Penal antes da sistematização do tema, culminada pelo Pacote Anticrime.

Não se pode deixar de mencionar que a doutrina afirma que há uma:

> [...] presunção relativa de regularidade da prova. Mesmo nos Estados Unidos da América, de onde se importou o instituto da Cadeia de Custódia, prevalece o entendimento de que se um elemento de prova estava custodiado por uma instância oficial do governo, "há uma presunção de regularidade da evidência e de que o funcionário público se desincumbiu com êxito seu dever legal de guardá-la sem permitir seu indevido manejo" (Magno; Comploier, 2021, p. 208).

Além disso, significativo destaque merece a afirmação de Magno e Comploier (2021, p. 208), que no tocante à necessidade da Cadeia de Custódia:

> a cadeia de custódia é apenas uma das maneiras de autenticar uma evidência, havendo também outras diversas possibilidades de autenticação. Deste modo, nem sempre a prova da cadeia de custódia lá é necessária (Magno; Comploier, 2021, p. 208).

A análise da doutrina também nos traz a ideia de que a prova da cadeia de custódia da prova é uma:

> metaprova, uma prova de segundo grau, ou seja, é uma prova acerca da atividade probatória. Por esse raciocínio, a metaprova não deixa de ser uma prova, o que exigiria outra prova – e assim sucessivamente, desembocando no problema do regresso infinito que passaria a existir sobre a atividade probatória (MAGNO; COMPLOIER, 2021, p. 210).

Magno e Comploier prosseguem o raciocínio sustentando, em virtude do apresentado bem como devido a outras razões, que:

> não cabe à acusação apresentar sempre e em todos os casos a prova de cadeia de custódia da prova. Para que o valor da prova seja relativizado e seja apresentada uma contraprova da acusação que demonstre a documentação detalhada da cadeia de custódia, faz-se necessário que a defesa apresente indicações mínimas de adulteração, manipulação ou contaminação da evidência (2021, p. 210).

De qualquer forma, o legislador achou por bem estabelecer a normatização, à exaustão, de todo o procedimento da Cadeia de Custódia, reconhecendo-a no âmbito da codificação infraconstitucional brasileira, vinculando assim, todo o sistema processual penal a partir da alteração e entrada em vigor dos novos artigos do CPP.

3 EVIDÊNCIAS DIGITAIS

A era da informação trouxe uma transformação significativa na forma como os crimes são cometidos e investigados. O advento das tecnologias de informação e comunicação gerou um aumento significativo na quantidade e na variedade de dados digitais.

Esses dados, que incluem e-mails, mensagens instantâneas, registros de chamadas, dados de localização, informações armazenadas em nuvem, logs de sistemas, vídeos, imagens

digitais, entre outros, se tornaram cruciais em investigações criminais, constituindo-se "evidências digitais".

Nassif aponta (2019, p. 91): "uma evidência digital pode ser aceita em um tribunal desde que permaneça confiável desde a sua apreensão". Assim, evidências digitais compreendem "qualquer informação de valor probatório que seja armazenada ou transmitida em formato digital" (Nassif, 2019, p. 92).

Fernandes e Montes (2022, p. 60-61) tratam sobre a caracterização da evidência digital:

> esses arquivos digitais nada mais são do que documentos, porém de forma eletrônica, diferentemente dos documentos no formato físico, onde as informações são inscritas em papel e, portanto, tangíveis, os documentos eletrônicos não são palpáveis. Não obstante esses documentos físicos possam tornar-se digitais, através de uma fotografia ou um escaneamento, ainda assim seu meio de produção é físico. Por outro lado, aqueles (eletrônicos), estão dissociados de uma plataforma física única de armazenamento. Esses arquivos digitais por vezes trafegam armazenados entre diversos dispositivos eletrônicos –DVDs, pen-drives, HDs, plataformas remotas (*cloud storage*). Ou seja, o documento digital não está preso a um único e distinto meio físico.

Lucien (2023, p. 40) também apresenta como a prova digital pode ser conceituada ou caracterizada:

> prova digital não é nada mais nada menos que todo e qualquer dado que esteja armazenado ou que seja transmitido via computador e sirva para apoiar ou para rejeitar alguma teoria sobre como um crime específico aconteceu e que contenha elementos críticos desse crime, como intenção ou álibi.

Cada tipo de evidência digital apresenta características únicas que modificam a forma de sua coleta e preservação.

Acerca da diferença de manuseio para extração de dados de dispositivos digitais:

> Diferentemente da abordagem de aquisição de dados em ambientes computacionais, em que geralmente os dados podem ser extraídos no estado em que foram encontrados e ficam preservados a partir do momento da sua apreensão, a extração de dados de telefones celulares e smartphones normalmente exige a execução de alguma intervenção no dispositivo. Além disso, tendo em vista que utilizam memórias embutidas, cujo acesso, sendo direto ao hardware, é delicado e complexo, é preciso instalar aplicativos ou utilizar ferramentas diretamente no dispositivo para que se proceda à aquisição dos dados armazenados e consequentes evidências. (Simão; Sícoli; Melo; Deus; Sousa Júnior, 2011, p. 93).

Como apontado por Simão e outros (2011), a coleta e análise de evidências digitais exigem uma compreensão profunda das tecnologias utilizadas e dos métodos forenses para preservar a integridade dos dados. A complexidade técnica das evidências digitais impõe a necessidade de peritos especializados:

> o analista pericial deve ter o conhecimento necessário para realizar os procedimentos periciais no dispositivo da forma menos intrusiva possível, controlando o ambiente de maneira a se evitar a perda, a alteração ou mesmo a contaminação de dados tratados como evidências, o que dará maior confiabilidade à perícia. (Simão; Sícoli; Melo; Deus; Sousa Júnior, 2011, p. 93).

A complexidade das investigações envolvendo dispositivos eletrônicos ressalta a necessidade crítica de um processo bem definido para coletar e extrair evidências digitais. Como destacado por Nassif (2019, p. 89):

> A investigação de crimes que utilizam dispositivos eletrônicos exige um mecanismo adequado de coleta e extração dessas evidências. Se o investigador ou policial não apreende provas digitais de forma a serem usadas em um processo forense, algumas informações importantes podem ser perdidas, e os juízes podem descartar provas do caso porque a apreensão ou a extração foram inadequadas. A correta apreensão de forense digital envolve a preparação de profissionais das áreas de direito, de segurança policial e de informática.

A necessidade de garantir a autenticidade e integridade dos documentos digitais é equiparada à segurança exigida pelos documentos físicos, como destacam Fernandes e Montes (2022, p. 61):

> assim como ocorre com os documentos físicos em papéis, através de assinaturas e certidões que garantem a sua autenticidade e a sua integridade, aos documentos digitais não é diferente. Surge então a necessidade de garantir aos documentos digitais as mesmas garantias de veracidade da prova que existem nos documentos físicos.

Em conformidade com o artigo 158-A do Código de Processo Penal (CPP), a perícia deve ser conduzida de maneira a assegurar a imparcialidade e a precisão das provas apresentadas. Isso é especialmente relevante para evidências digitais, onde a manipulação ou alteração de dados pode comprometer toda a investigação.

A importância de garantir a credibilidade dos vestígios digitais ao longo das etapas da persecução penal é destacada por Fernandes e Montes (2022, p. 61):

> É imprescindível que todos os procedimentos de documentação realizados com os vestígios digitais visando a preservação de sua credibilidade em todas as etapas da persecução penal permitam a concretização dos princípios basilares do contraditório e da ampla defesa, uma vez que controlam a atuação estatal sobre aquilo que será fonte de prova.

O uso de evidências digitais requer que elas estejam em conformidade com, ao menos, dois princípios: a autenticidade, que seria a propriedade essencial, asseguradora de que os fatos ali dispostos estão de acordo com o fato jurídico ocorrido e que foram praticados pelos seus respectivos autores; e a integridade, que é a garantia de que a evidência não sofreu qualquer adulteração desde sua coleta. (Lucien, 2023, p. 40).

Lucien (2023, p. 40) esclarece que, em razão desses atributos - autenticidade e integridade – "ratifica-se a importância da presença de especialistas que detenham densos conhecimentos nas áreas de Direito Digital e perícia forense digital em casos dessa natureza, com vistas a evitar a contaminação ou a anulação da prova coletada".

Como vimos, a cadeia de custódia é um conceito fundamental para garantir a integridade das provas, assegurando que qualquer evidência coletada seja adequadamente documentada, armazenada e manuseada até sua apresentação em tribunal.

Para as evidências digitais, a cadeia de custódia envolve procedimentos específicos que começam com a coleta de dados em um ambiente forense controlado. Cada etapa, desde a coleta até a análise e armazenamento, deve ser documentada minuciosamente. A manutenção de logs detalhados que registrem quem teve acesso às evidências, quando e por qual motivo, é crucial para garantir que não haja contaminação ou adulteração dos dados:

> No âmbito digital, a simples coleta de evidências sem utilização de técnica adequada pode eliminar todas as chances do litígio judicial, devido à contaminação do local do crime. Da mesma forma, ocorre com a coleta sem o emprego de manutenção e de registro histórico cronológico das evidências (cadeia de custódia), haja vista a possibilidade de a parte contrária argumentar sobre as evidências terem sofrido adulterações durante seu manuseio. (Lucien, 2023, p. 41).

Segundo a norma ISO/IEC 27027/2013, os principais procedimentos para identificação, coleta e aquisição da evidência digital são: "cadeia de custódia, pessoal, potencial evidência digital, documentação, instruções, evidência digital específica, coleta ou aquisição e preservação da evidência digital".

A necessidade de padronização no tratamento das evidências digitais para garantir sua integridade e autenticidade é enfatizada por Lucien (2023, p. 42):

> Ante a fragilidade da evidência digital, o tratamento para assegurar sua integridade e autenticidade deve ser padronizado. E os principais elementos que possibilitam a credibilidade da investigação são: qualificação das pessoas para execução das tarefas e aplicação de metodologia adequada. O primeiro se refere a 42 interventores – pessoas com conhecimento suficiente para auxílio no manuseio de evidência digital – e a especialistas – indivíduos com grande experiência e condição de assegurar sua preservação; o segundo, à norma que padroniza o tratamento de evidências digitais em todas as etapas do processo.

Em relação às alterações introduzidas pelo "Pacote Anticrime", Lei nº 13.964, de 2019, em especial as disposições relacionadas com a cadeia de custódia dos vestígios, o principal objetivo dessas alterações é a manutenção e a documentação da cronologia do vestígio criminoso, como possibilidade de rastrear sua posse e manuseio, bem como seu curso seguinte até o descarte (MPPR, 2016, p. 290 apud Lucien, 2023, p. 42).

Ocorre que é o legislador descreveu a cadeia de custódia das provas físicas, mas não tratou dos procedimentos referentes à custódia de evidências digitais, as quais tem se tornado comum devido ao aumento da ocorrência de cibercrimes na "era da sociedade da informação".

Lucien (2023, p. 42) aponta essa problemática e destaca que a evidência digital "colocou o processo penal diante de um problema jurídico em relação à possível adaptação dos meios tradicionais de prova às novas tecnologias". Ela esclarece como o avanço tecnológico confronta o processo penal com novos desafios, como o acesso transfronteiriço a dados, acesso remoto e uso de software malicioso pelo Estado, todos considerados meios de prova modernos. Destaca a complexidade do exame jurídico envolvido e a necessidade de discussões aprofundadas, sempre pautadas pela proteção das garantias constitucionais, especialmente o direito à privacidade, e pela garantia da certeza do elemento probatório através da cadeia de custódia. O progresso tecnológico, segundo ela, demanda uma revisão abrangente dos conceitos legais e garantias para adaptá-los ao novo paradigma social, assegurando uma proteção eficaz e uma resposta satisfatória no âmbito jurídico.

Há, então, uma lacuna que deve ser suprida "devido a possíveis prejuízos processuais que possam ocorrer, como inadmissibilidade ou exclusão de provas digitais dos autos ou até redução da força probatória" (Lucien, 2023, p. 42).

Não obstante, enquanto a omissão não é suprida, a observância da cadeia de custódia deve prevalecer em relação às evidências digitais, uma vez que a ideia de cadeia de custódia e preservação da prova existe mesmo antes da positivação do termo. É inafastável do conceito de "prova" a manutenção de sua autenticidade, integridade, rastreabilidade, confiabilidade, que são atributos inerentes à validade/licitude da prova.

A prova pericial e a cadeia de custódia são pilares fundamentais na investigação de todos os crimes, mas no âmbito dos crimes digitais possuem especial relevância, uma vez que tais crimes são comumente mais complexos e a prova pericial pode ser fortemente aliada à identificação dos indícios de autoria e materialidade dos cibercrimes. A complexidade e a variabilidade das evidências digitais demandam abordagens especializadas e rigorosas para sua coleta, preservação e análise. A integridade do processo judicial depende da qualidade das práticas forenses empregadas e da observância à cadeia de custódia prevista pelo Código de Processo Penal.

Ademais, como vimos, a formação e a qualificação de profissionais especializados em Direito Digital e perícia forense digital são imperativas para superar os desafios atuais e futuros, assegurando que as evidências digitais sejam coletadas, preservadas e apresentadas de maneira que atendam aos mais altos padrões de precisão e imparcialidade, bem como para enfrentar os desafios e garantir a justiça em um mundo cada vez mais digitalizado.

CONCLUSÃO

A prova pericial tem um papel crucial na investigação e resolução de crimes, sendo essencial para a administração da justiça. Qualquer que seja sua origem, deve ser cuidadosamente produzida para ser considerada válida e, assim, subsidiar de maneira substancial e inequívoca as decisões judiciais na busca pela verdade real, como tradicionalmente estabelecido pelo Código de Processo Penal (CPP).

Essa qualidade em termos de inviolabilidade é garantida por uma série de procedimentos conhecida como cadeia de custódia, cujo principal objetivo é assegurar a integridade dos objetos e bens coletados pela perícia ou apreendidos pelas autoridades policiais durante a investigação criminal e o processo judicial subsequente, eliminando qualquer dúvida quanto à sua origem e ao trajeto percorrido.

Vimos que, até 2019, a cadeia de custódia situava-se no âmbito das "boas práticas" em perícia, sem uma normatização efetiva que regulasse seu procedimento. Reconhecendo a necessidade de regulamentação exaustiva e precisa, o legislador decidiu estabelecer uma normatização abrangente de todo o procedimento da cadeia de custódia. Essa normatização foi integrada ao sistema de codificação infraconstitucional brasileira, vinculando todo o sistema processual penal. A alteração e entrada em vigor dos novos artigos do Código de Processo Penal (CPP) reforçaram a importância da cadeia de custódia, garantindo que todas as etapas do processo sejam conduzidas de acordo com diretrizes claras e estabelecidas legalmente.

Conforme análise realizada, constatamos que no contexto dos crimes digitais, a importância da prova pericial é ainda mais acentuada, dada a complexidade e a natureza técnica dos cibercrimes e das evidências envolvidas. A correta coleta, preservação e análise dessas evidências são fundamentais para garantir a integridade do processo judicial.

Evidências digitais apresentam características únicas em comparação com evidências físicas tradicionais. Diferentemente de objetos tangíveis, dados digitais podem ser facilmente

alterados, deletados ou copiados sem deixar vestígios aparentes. A volatilidade das evidências digitais requer um manejo extremamente cuidadoso e técnicas especializadas para garantir sua integridade. Além disso, a natureza intangível dos dados digitais faz com que a comprovação de sua autenticidade dependa fortemente da tecnologia utilizada e dos procedimentos seguidos na sua obtenção e análise.

A despeito da evolução legislativa relacionada com a normatização da cadeia de custódia, o legislador descreveu a cadeia de custódia das provas físicas, mas não tratou dos procedimentos referentes à custódia de evidências digitais. Entendemos, por outro lado, que a observância da cadeia de custódia deve prevalecer em relação às evidências digitais, uma vez que a ideia de cadeia de custódia e preservação da prova existe mesmo antes da positivação do termo. É inafastável do conceito de "prova" a manutenção de sua autenticidade, integridade, rastreabilidade, confiabilidade, que são atributos inerentes à validade/licitude da prova.

Em suma, após o estudo realizado, foi possível responder ao problema de pesquisa, qual seja: Quais são os principais desafios relacionados com as evidências digitais e como esses desafios influenciam a integridade e admissibilidade das provas no sistema judiciário brasileiro após a introdução do "Pacote Anticrime"?

Identificamos que a complexidade técnica na coleta e análise das evidências digitais, a fragilidade das evidências que podem ser facilmente manipuladas e contaminadas, bem como a lacuna na regulamentação específica para a custódia das evidências digitais, são alguns dos principais desafios relacionados com a temática. Esses desafios podem influenciar diretamente a integridade e a admissibilidade das provas no sistema judiciário. A integridade das provas é fundamental para assegurar um julgamento justo, e qualquer falha na preservação ou na documentação das evidências pode resultar na sua exclusão ou na diminuição de sua força probatória. Portanto, para que as evidências digitais sejam plenamente integradas ao processo judicial, é crucial a observância estrita à cadeia de custódia. Adicionalmente, a implementação de infraestrutura adequada e de especialização dos peritos, bem como, a supressão da lacuna existente, são fatores que podem contribuir com a minimização de problemas relacionados com a integridade das evidências digitais.

A prova pericial e a cadeia de custódia são pilares fundamentais na investigação de todos os crimes, mas no âmbito dos crimes digitais possuem especial relevância, uma vez que tais crimes são comumente mais complexos e a prova pericial pode ser fortemente aliada à

identificação dos indícios de autoria e materialidade dos cibercrimes. A complexidade e a variabilidade das evidências digitais demandam abordagens especializadas e rigorosas para sua coleta, preservação e análise. A integridade do processo judicial depende da qualidade das práticas forenses empregadas e da observância à cadeia de custódia prevista pelo Código de Processo Penal. A contínua evolução tecnológica e a colaboração interdisciplinar são essenciais para enfrentar os desafios e garantir a justiça em um mundo cada vez mais digitalizado.

REFERÊNCIAS

BRASIL. Código de Processo Civil**. Decreto Lei No 13.105, de 16 de março de 2015**. Diário Oficial da União Brasília, DF, 16 mar. 2015. Disponível em: https://presrepublica.jusbrasil.com.br/legislacao/174276278/lei-13105-15. Acesso em 14 jun.2024.

BRASIL. Código de Processo Penal. **Decreto Lei No 3.689, de 03 de outubro de 1941**. Diário Oficial da União - Seção 1, p. 19.699, Brasília, DF, 13 out. 1941. Disponível em: https://www2.camara.leg.br/legin/fed/declei/1940-1949/decretolei-3689-3-outubro-1941-322206-publicacaooriginal-1-pe.html. Acesso em 14 jun.2024.

BRASIL**. Lei Nº 13.964, de 24 de dezembro de 2019**. Aperfeiçoa a legislação penal e processual penal. Diário Oficial da União, Brasília, DF, 29 abr. 2021. Disponível em: https://legislacao.presidencia.gov.br/atos/?tipo=LEI&numero=13964&ano=2019&ato=8cfATVE5keZpWT929. Acesso em: 10 maio 2021.

BRASIL. Secretaria Nacional de Segurança Pública. **Portaria n.º 82, de 16 de julho de 2014**. Estabelece as Diretrizes sobre os procedimentos a serem observados no tocante à cadeia de custódia de vestígios. Diário Oficial da União, Brasília, DF, 18 julho, 2014.

BRÁZ, J. **Investigação criminal: a organização, o método e a prova: os desafios da nova criminalidade**. Coimbra: Almedina, 2019.

CINTRA, A.C.A.; GRINOVER, A.P.; DINAMARCO, C.R. **Teoria Geral do Processo**. 17. ed. São Paulo: Malheiros, 2001.

COLÔMBIA. **Ley 906 de 2004. Código de Procedimiento Penal Colombiano.** Publicada no Diário Oficial número 45.657 de 31 de agosto de 2004. Disponível em: http://www.secretariasenado.gov.co/senado/basedoc/ley_0906_2004.html. Acesso em: 10 maio 2020.

CROCE, D.; CROCE JÚNIOR, D. **Manual de Medicina Legal**. 6. ed. rev. São Paulo: Saraiva, 2009.

ESPÍNDULA, A. **Perícia criminal e cível: uma visão geral para peritos e usuários da perícia**. 3. ed. Campinas, São Paulo: Millennium Editora, 2009.

FERNANDES, André Luis. MONTES, Rodrigo Henrique de Oliveira. Meta-evidência digital: a dualidade na cadeia de custódia envolvendo dispositivos eletrônicos e evidências digitais. **Revista Eletrônica Direito & TI**, Porto Alegre, vol. 1, n. 14, dez. 2022.

GIACOMOLLI, N. J.; AMARAL, M. E. A. A cadeia de custódia da prova pericial na Lei Nº 13.964/2019. **Revista Duc In Altum,** Cadernos de Direito, v. 12, n. 27, p. 67–99, 2020.

GONZÁLEZ, R. D. A. **Cadena de Custodia en Criminalística**. Bogotá: Ediciones Doctrina y Ley, 2016.

MAGNO, L. E.; COMPLOIER, M. Cadeia de custódia da prova penal. **Cadernos Jurídicos, Escola Paulista da Magistratura**, São Paulo, v. 22, n. 57, p. 195-219, jan./mar. 2021. Disponível em: https://www.tjsp.jus.br/download/EPM/Publicacoes/CadernosJuridicos/cj_n57_10_cadeia%20de%20. Acesso em 14 jun.2024.

NASSIF, Lilian Noronha. Desafios da coleta de dados e em evidências digitais. **O Alferes**, Belo Horizonte, 74 (29): 89-107, jan./jun. 2019.

PIERANGELI, J. H. Processo penal. **Evolução histórica e fontes legislativas**. São Paulo: Editora Jalovi, 1983.

ROSA, M. S.; IRIBURE JÚNIOR, H. C. Relativização da Presunção de Inocência sobre o Prisma da Integridade e Coerência de Ronald Dworkin**. Revista de Direito Penal, Processo Penal e Constituição**, Salvador, v. 4, n. 1, p. 45-67, jan./jul. 2018. Disponível em: https://www.indexlaw.org/index.php/direitopenal/article/view/4019/pdf. Acesso em 14 jun.2024.

SILVA, A. A. G. da. **A Perícia Forense no Brasil**. 2010. Dissertação (Mestrado em Engenharia Elétrica) - Escola Politécnica, Universidade de São Paulo, São Paulo, 2010.

SILVA, W. C. da. **O princípio da presunção de inocência ou não culpabilidade**. Jus.com, [S. l.], fev. 2018. Disponível em: https://jus.com.br/artigos/64135/oprincipio-da-presuncao-de-inocencia-ou-nao culpabilidade. Acesso em 14 jun.2024.

SIMÃO, A. M. L. SÍCOLI, F. C. MELO, L. P. DEUS, F. E. D. SOUSA JÚNIOR, R. T. **Aquisição de evidências digitais em Smartphones Android**. ICOFCS. 2011. DOI: http://dx.doi.org/10.5769/C2011009.

TAVARES, A. A. G; ANDRADE, O. DE O. ANDRADE. Pressupostos constitucionais da prova pericial no processo penal. **Revista de Ciências Jurídicas e Sociais**, 3(1), 7-17 (2013).

7 Information Society and Law
FMU CENTRO UNIVERSITÁRIO

USO DA INTELIGÊNCIA ARTIFICIAL PARA CRIAÇÃO DE CONTEÚDO SEXUAL INFANTIL: A EXPANSÃO DA PEDOFILIA VIRTUAL

USING ARTIFICIAL INTELLIGENCE TO CREATE CHILD SEXUAL CONTENT: THE EXPANSION OF VIRTUAL PEDOPHILIA

Mariana Pereira Marques[1]

Resumo: Este artigo propõe uma análise da utilização indevida dos meios tecnológicos para criação de conteúdo sexual com crianças e adolescentes. Com base em um estudo analítico da legislação brasileira, jurisprudências, projetos de leis e doutrinas. O principal objetivo deste artigo é a informação e a conscientização de pais, responsáveis e adolescentes sobre o elevado índice de cibercrimes cometidos contra crianças e adolescentes. Secundariamente, será pontuado acerca do tratamento dado pelas leis brasileiras nestes casos e sua caminhada para a criminalização.
Palavras-Chave: Inteligência Artificial; Cibercrime; *Deepfake*.

Abstract: This article proposes an analysis of the misuse of technological media to create sexual content with children and teenagers. Based on an analytical study of brazilian legislation, case law, draft legislation and doctrine. The main aim of this article is to inform and raise awareness among parents, guardians and teenagers about the high rate of cybercrime committed against children and teenagers. Secondly, it will discuss the treatment given by brazilian law to these cases and their path towards criminalization.
Keywords: Artificial Intelligence; Cybercrime; Deepfake.

INTRODUÇÃO

É imprescindível iniciar com o significado da palavra “comunicação”, que é a “ação de transmitir uma mensagem e, eventualmente, receber outra mensagem como resposta”. Tal necessidade cresceu da ideia de que a *internet*, após inúmeros avanços tecnológicos e adaptações dos seres humanos, foi crucial para facilitar a transmissão de mensagens, não só como meio de conversa, mas também como fonte de informação. A comunicação se tornou muito mais eficaz e veloz, tendo em vista que longas distâncias não eram mais um obstáculo para diálogos, ou um empecilho para jovens com anseio por conhecimento.

[1] Graduanda em direito pelas Faculdades Metropolitanas Unidas – FMU, com previsão de término para dezembro de 2025.

Um dos meios essenciais para a confabulação das pessoas ainda se encontra nas redes sociais, como *Instagram, Facebook*, entre tantas outras. Porém, o consumo excessivo destas, e pior, por meio de exposição, trouxe inúmeros malefícios. Problemas psicológicos, como ansiedade e depressão, por não terem a vida que queria ou que outra pessoa, aparentemente, tem; problemas físicos pela falta de postura ao utilizar o celular ou por usá-lo por muito tempo e não praticar qualquer atividade física.

Problemas reais com consequências reais que, infelizmente, crianças e adolescentes não estão exclusos. E mais, são os alvos centrais de pessoas mal-intencionadas neste meio.

Este artigo visa, como objetivo principal, trazer um estudo analítico de observação entre a exposição excessiva nas redes sociais e suas consequências na vida das crianças e adolescentes no âmbito do *cyberbullying*, a partir do uso de inteligência artificial para a confecção de imagens pornográficas falsas.

Os objetivos secundários são conceituar *cyberbullying e deepfake*, identificar a legislação brasileira pertinente e pontuar os principais casos que ocorreram atualmente.

1. LEGISLAÇÃO PERTINENTE

1.1. Princípios do direito penal

Antes de tudo, é necessário explicar o que é GDPR e quais são suas implicações no direito brasileiro e, principalmente, quando se trata de uso de dados pessoais. GDPR é uma sigla em inglês para "Regulamento Geral sobre a Proteção de Dados", um projeto idealizado em 2012 e aprovado em 2016 na União Europeia com o objetivo de proteger os dados e a identidade de seus cidadãos.

Quanto ao Brasil, não só foi fundamental para a criação da Lei Geral de Proteção de Dados, lei nº 13.709/2018, mas também na área comercial, haja vista que toda empresa com interesse em exportar seus produtos para a União Europeia, deverá adaptar-se ao regulamento pertinente. Pela praticidade, é comum ver as empresas atualizando seus sistemas e termos, pois atuam globalmente e querem evitar riscos, como de infringir alguma lei.

Tendo em vista estas informações, quanto aos princípios norteadores do GDPR, são eles: licitude, lealdade, transparência, limitação da finalidade, minimização dos dados, exatidão, limitação da conservação, integridade e confidencialidade (que são os mesmos da segurança da informação), e responsabilidade.

Já a LGPD, em seu artigo 6º, descreve seus princípios norteadores, que são: da finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas.

Conforme estudos de Luciana Cristina e Licia (2020, p. 194), "os princípios gerais de proteção de dados foram elaborados e expressamente previstos na lei devendo ser interpretados principalmente em benefício do titular de dados que é a parte vulnerável sobre diversos ângulos", assim sendo, utilizar dados, pessoais ou sensíveis, de maneira não condizente à informada pelo usuário, ou ainda, sem qualquer conhecimento deste, implicará em penalidades.

Ademais, vale indicar que a segurança e tratamento adequado dos dados fornecidos deve caminhar em consonância com a conscientização das pessoas, repassando somente as informações essenciais à situação e observando as políticas da empresa. Em caso de insegurança ou dúvida, procure ajuda e não diga nada.

1.2. Lei geral de proteção de dados – LGPD

Crianças e adolescentes têm seus dados pessoais tratados de maneira diferenciada, vez que são menores de idade e devem obter o consentimento de um dos pais ou responsáveis legais para fornecerem tais informações, porém, no artigo 14 da LGPD, § 3º, é possível verificar uma exceção:

> § 3º Poderão ser coletados dados pessoais de crianças **sem o consentimento a que se refere o § 1º deste artigo** quando a coleta for necessária para contatar os pais ou o responsável legal, **utilizados uma única vez e sem armazenamento**, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º deste artigo. (Brasil, 2018, grifo nosso).

Como é possível compreender da leitura do artigo completo, o legislador teve a preocupação de respeitar, essencialmente, os princípios da finalidade e transparência, pois o meio digital tem inúmeras formas de burlar o sistema de identificação e, portanto, o uso indevido de dados pessoais de menores de idade pode ocorrer de maneira generalizada e desenfreada, podendo ocasionar, em maiores níveis, traumas de origem física, moral e psicológicas irreversíveis. Para tanto, é necessário que os controladores[2] verifiquem sempre se o consentimento requerido é real e válido.

[2] Conforme inciso VI, artigo 5º da lei nº 13.709/2018, é a "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais".

Ainda, vale mencionar que, com a propagação do uso de inteligência artificial, não só os dados já fornecidos pelos petizes são utilizados de maneira indevida, mas também um conteúdo completamente novo é criado a partir do absoluto nada, apenas pelo desejo e comando do usuário.

1.3. Estatuto da criança e do adolescente – ECA

Observando o Estatuto da Criança e do Adolescente sob o espectro da coleta e proteção de dados, tal legislação aborda o tema, em linhas gerais, em seus primeiros artigos, nas disposições preliminares, como:

> Art. 4º É dever da família, da comunidade, da sociedade em geral e do poder público **assegurar, com absoluta prioridade**, a efetivação dos direitos referentes à vida, à saúde, à alimentação, à educação, ao esporte, ao lazer, à profissionalização, à cultura, à dignidade, ao respeito, à liberdade e à convivência familiar e comunitária.
> Parágrafo único. A garantia de prioridade compreende:
> [...]
> d) destinação privilegiada de recursos públicos nas áreas relacionadas com a **proteção à infância e à juventude**.
> Art. 5º **Nenhuma criança ou adolescente será objeto de qualquer forma de negligência, discriminação, exploração, violência, crueldade e opressão**, punido na forma da lei qualquer atentado, por ação ou omissão, aos seus direitos fundamentais. (Brasil, 1990, grifo nosso).

Ao ler os artigos supra é possível identificar similaridades com outros artigos de outras leis, como a própria Constituição Federal, em seus artigos 227 e 229.

Também na Lei nº 12.965/2014, conhecida como Lei do Marco Civil da *Internet*, em seu artigo 29, é possível enxergar a conexão, tendo em vista que o controle exercido pelos responsáveis legais do menor no que ele poderá acessar na *internet* é uma forma de proteção, vejamos:

> Art. 29. O usuário terá a opção de livre escolha na utilização de programa de computador em seu terminal **para exercício do controle parental de conteúdo entendido por ele como impróprio a seus filhos menores, desde que respeitados os princípios desta Lei e da Lei nº 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente**.
> Parágrafo único. Cabe ao poder público, em conjunto com os provedores de conexão e de aplicações de internet e a sociedade civil, promover a educação e fornecer informações sobre o uso dos programas de computador previstos no caput, bem como para a definição de boas práticas para a inclusão digital de crianças e adolescentes. (Brasil, 2014, grifo nosso).

Assim sendo, tem-se que, não só os pais, mas toda a sociedade são responsáveis por criar e manter o ambiente digital seguro para os menores, tendo em vista seus direitos protegidos

por várias legislações e os princípios morais basilares para assegurar as boas relações em comunidade, tanto pessoalmente quanto digitalmente.

Quanto aos crimes que podem ser cometidos, o ECA define em seus artigos que é proibido:

> Produzir, reproduzir, dirigir, fotografar, filmar ou registrar cenas de sexo (Art. 240); Vender fotografias, vídeos ou outros registros sexuais (Art. 241); Distribuir ou divulgar de qualquer forma cenas de sexo explícito ou pornografias (241 – A); Adquirir ou armazenar mídias envolvendo pornografia (241 – B); Fazer montagens (manipulação de imagens, vídeos…) envolvendo cenas com conotação sexual (241 – C); Aliciar, assediar, instigar ou constranger através de qualquer meio com fim de praticar atos libidinosos (241 – D). (Brasil, 1990).

E, como veremos, além da exposição excessiva de menores nas redes sociais, o uso indevido de inteligências artificiais contribui diretamente para o ramo dos cibercrimes.

1.4. Projeto de lei nº 5.694/2023

Por proposta realizada pelo deputado pastor Eurico – que, atualmente, segue para a Comissão de Previdência, Assistência Social, Infância, Adolescência e Família (CPASF) –, o Projeto de Lei n° 6.694 de 2023 prevê criminalizar "a manipulação ou adulteração de fotos, vídeos ou sons, utilizando-se de sistemas de inteligência artificial", incluindo o aumento da pena para crimes relacionados à pornografia infantil.

Sendo aprovada a lei, a imprecisão de norma para casos como estes terão amparo legal especificamente pontuado e, assim, trazendo maior segurança jurídica aos julgados neste sentido, havendo amparo a vítima e justa punição ao infrator.

2. A EXPOSIÇÃO DE CRIANÇAS ÀS REDES SOCIAIS E SUA CONTRIBUIÇÃO DIRETA PARA A PROPAGAÇÃO DA PEDOFILIA VIRTUAL

Ao postar uma foto de uma criança, por mais que, na opinião de pais e familiares, a foto é tida por "fofinha", "ingênua" e "transmita pureza", no outro lado da tela há alguém que não irá ver da mesma forma e, então, já será tarde demais. Através de publicações feitas pelos pais, os criminosos têm acesso a informações crucias para o planejamento do crime, como: a rotina da criança; quem cuida da criança, se são os pais ou a babá; a escola em que estuda; as atividades extracurriculares; os desenhos, músicas e alimentos que gosta, entre outras. E por mais que pareçam insignificantes, essas são apenas algumas informações que podem induzir seus filhos a seguir os criminosos.

No ano de 2014, em Santa Catarina, houve um caso em que o réu planejou o sequestro de um menino de 09 anos apenas com as informações que conseguiu através das publicações feitas pelos pais da criança em seu *Facebook*.

Em depoimento, o criminoso disse o seguinte: "No Facebook mostra tudo. Foi coisa de [planejei em] 10 dias, no máximo. Se vocês puxarem lá vão ver como mostra tudo da vida pessoal. Mostra até dentro da casa deles" (MACHADO, Peterson da Silva, 2014). Se apenas com publicações feitas pelos pais oferecem todas as informações necessárias para a consumação de um sequestro, as mesmas publicações oferecem o material perfeito para crimes cibernéticos.

A simples foto de uma criança com roupas de banho (biquini, maiô, sunga ou bermuda) pode se tornar o pior pesadelo na vida dos pais. Indivíduos podem, simplesmente, fazer uma *deepfake* da criança, entendendo este termo como as imagens geradas por inteligência artificial, onde os criminosos pegam fotos de qualquer criança, inclusive de casos de pedofilia, e fazem uma edição, colocando-a em situações de exploração ou abuso sexual e, depois, distribuindo entre pedófilos na *dark web*.

Segundo pesquisa realizada pela SaferNet, a quantidade de imagens de abuso e exploração sexual infantis encontradas em âmbito virtual cresceu em 70% no primeiro quadrimestre de 2023, sendo a maior alta desde 2020.

Agora, passando para um cenário mais habitual, temos os crimes de difamação e injúria (artigos 139 e 140 do Código Penal), que são os mais comuns de se encontrar em âmbito digital, porém estão "disfarçados" pela opinião e liberdade de expressão das pessoas.

Em rápida definição: difamar é tirar a boa fama ou o crédito, desacreditar publicamente, atribuindo a alguém um fato específico negativo. Para ocorrência deste, o fato atribuído não pode ser considerado crime. Contudo, o crime de injúria é atribuir palavras ou qualidades ofensivas a alguém, expor defeitos ou opinião que desqualifique a pessoa, atingindo sua honra e moral.

Apesar de parecer absurdo, esses dois crimes são cometidos contra crianças e bebês a todo instante, e os filhos de influenciadores digitais e famosos são os principais alvos, pois tem suas vidas expostas desde que nascem e muitos sentem-se na liberdade e direito de "opinar" sobre.

Assim, vejamos alguns exemplos:

- Em outubro 2022, logo após seu nascimento, Maria Flor, filha de Virginia Fonseca e Zé Felipe, foi atacada por sua aparência: “q criança feia essa maria flor deus q me perdoe”;
- Em julho de 2023, Aurora (10 meses), filha de Pedro Scooby e Cíntia Dicker, foi atacada quando tinha 6 meses, por sua aparência: “parece que tem problema”;
- Em 2023, Lua (7 meses), filha de Viih Tube e Eliezer, é atacada desde seus três meses por conta de seu corpo: “Do que adianta nascer rica, mas ser obesa?”; “Tinha tudo pra ser linda, mas é obesa. Tadinha”, “Ela vai explodir”;
- Em 2023, Luca (9 meses), filho de Claudia Raia e Jarbas Homem de Mello, é atacado por conta de seu corpo: “É uma gracinha. Mais muito magro. Essa criança precisa é de massa"; "Acho que o seu leite, não está suficiente para ele. Que tal complementar com um leite específico?"; "Nossa, tadinho! Muito magro. Até os olhinhos estão esbugalhados! Tem de examinar ele e ver se está abaixo peso e suplementar"”;
- Em 2023, Phoenix (10 meses), filho de Paris Hilton e Carter Reum, foi atacado por internautas por conta do tamanho de sua cabeça: “*He thinking a lot* – ele está pensando demais”; “*This child could be hydrozephalus. Plz check* – essa criança deve ter hidrocefalia. Por favor examine”; “*Cuando me dicen que no piense demasiado las cosas* – quando me pedem para não pensar demais nas coisas”;

No dia 15 de novembro de 2023, o digital influencer Eliezer, em seu perfil do Instagram, informou aos seus seguidores que ele e sua esposa, Vitória (conhecida pelo codinome “Viih Tube”), junto a sua equipe de advogados, irão processar todas as pessoas que atacaram sua filha, Lua, além de informar aos seus seguidores o que pode ser feito em casos de ataques virtuais.

Em publicação o influencer disse o seguinte:

> O objetivo desse vídeo é INFORMAÇÃO! Se você já sofreu/sofre ou conhece alguém que é ofendido/xingado na internet e não faz nada porque acha que nada acontece com a pessoa, assista o vídeo e/ou compartilha.
> Todas as informações que têm nele NÃO são achismos nem tiradas da minha cabeça. É na prática o que QUALQUER PESSOA pode fazer (sendo pessoa pública ou não) quando é xingado/ofendido no Instagram. Eu juntei com a minha equipe de advogados (obrigado @drpedromansur e @mansurmarquesadv pelo tempo dedicado e todo esforço em fazer com que a lei seja cumprida) e fizemos esse “passo a passo” para vocês saberem o que fazer com as pessoas que te ofendem pagarem em juízo.
> A sensação de impunidade na internet é tão grande que todos os dias CRIMES continuam sendo cometidos de forma ininterrupta porque a maioria das pessoas acham que NADA pode ser feito. E isso é uma grande MENTIRA, porque pode sim! Diariamente pessoas são atacadas, humilhadas, menosprezadas na internet e não fazem nada porque acham que não tem nada pra fazer, MAS TEM! O que falta é informação, as pessoas saberem o que pode ser feito e como pode ser feito. As pessoas que cometem esses CRIMES só vão pensar 2 vezes antes de ofender ou xingar alguém quando serem condenados a pagarem uma grana pra quem ele/ela ofendeu ou até mesmo CADEIA!
> O vídeo NÃO é pra falar sobre a saúde da minha filha NEM para tentar convencer as pessoas a pararem com as ofensas e SIM para instruir e informar qualquer pessoa que EXISTE SIM uma maneira de parar essa pessoa que é fazendo ela te pagar e/ou indo preso. (2023).

Por fim, é importante ressaltar que, apesar das vítimas serem menores de idade, os pais e responsáveis podem, e devem, tomar as devidas providências legais, em conjunto com

organizações, estatais ou não, que prestem apoio e auxílio, em situações semelhantes, a todos os envolvidos. Assim, não só as vítimas vulneráveis serão tratas e conscientizadas, mas também seus responsáveis.

3. USO DE I.A. PARA CRIAÇÃO DE CONTEÚDO SEXUAL INFANTIL

Tendo como ponto de partida que a inteligência artificial executa algoritmos baseados em dados previamente informados ("The Alan Turing Institute", 2021), possibilitando a criação e evolução de máquinas cada vez mais tecnológicas e, principalmente, com consciência própria.

Assim, existe uma preocupação real por parte de grandes organizações globais, ensejando o desenvolvimento de recomendações e princípios para aplicação imediata, à título de exemplo: o primeiro padrão internacional, em 2019, constituindo as "Recomendações do Conselho de Inteligência Artificial". Porém, mesmo com tamanho zelo aos direitos humanos e valores democráticos, haveria efetividade em seus termos e justiça na prática?

Em pesquisa realizada pela McAfee, foi avaliado quão preocupados os pais são com a exposição dos filhos à *internet* e nesta etapa foi apontado que mais de 90% deles são "muito preocupados". Entretanto, por mais que exista esta preocupação, é impossível preveni-los de todo o mal que possa ser encontrado na *internet*. Segundo o Ministério dos Direitos Humanos, as crianças e os adolescentes são as maiores vítimas de crimes cibernéticos no Brasil.

No início de 2022 surgiu uma nova febre no Brasil, o famoso *BeReal*, a rede social do momento, que promete ser sem filtros, ou seja, mostrar o lado verdadeiro dos usuários. O aplicativo tem origem francesa e foi criado em 2020 por Alexis Barreyat., que a apresenta como uma rede social anti-*Instagram* e possui uma política "sem filtros", permitindo que o usuário faça apenas uma publicação por dia. O aplicativo emite um alerta e o usuário só tem 2 minutos para abri-lo e fazer uma fotografia, tirada instantaneamente da câmera frontal e traseira.

O *BeReal* não fez sucesso apenas no Brasil, mas mundialmente, como mostram os índices de 2022, quando obteve um marco de crescimento igual a 315% no período de dezembro de 2021 a maio de 2022. Ademais, no site "busniness app", foi divulgado em estáticas que o aplicativo, no mês de novembro de 2023, possui 25 milhões de usuários ativos. Porém, devido ao sucesso mundial, alguns profissionais começaram a pesquisar para entenderem melhor sobre o aplicativo, já os estudiosos passaram a estudar sobre essa nova sensação e encontraram uma lacuna na política de proteção de dados dos usuários. Quando instalado o aplicativo, o usuário

precisa concordar com os "Termos de Uso de Aplicativo e Política de Privacidade", onde autoriza o *BeReal* a "hospedar, armazenar, reproduzir, modificar, adaptar, exibir, publicar, editar, distribuir e sublicenciar todo ou parte do Conteúdo com a finalidade de fornecer os Serviços do Aplicativo aos seus Usuários e realizar atividades de marketing, comunicação ou promoção comercial" por 30 anos. Através dessa autorização de armazenamento de dados extremamente longa, a localização em tempo real e o livre acesso às câmeras do celular (frontal e traseira), temos um conjunto perfeito e completo para os criminosos. Fazendo uma analogia rápida, é como se déssemos a chave de nossas casas e uma arma na mão de criminosos para fazerem o que bem entenderem com nossas vidas e patrimônios.

Dessa forma, a exposição excessiva dos adolescentes às redes sociais não prejudica somente sua saúde física e mental, mas também sua segurança, tendo em vista que essa normalização de uma vida "sem filtros" para o *Instagram* facilita que criminosos consigam informações cruciais para elaboração de crimes. Além dos crimes comuns, contribui diretamente para o cibercrime, como a pedofilia virtual, *deepfakes*, *ciberbullying*, induzimento e instigação a automutilação e suicídio, entre outros.

A divulgação e confecção de *deepfakes* tem, infelizmente, adquirido cada vez mais força no universo cibernético, graças ao fácil acesso a ferramentas de inteligência artificial que, apenas com uma foto, consegue produzir imagens falsas de momentos íntimos.

Na edição do Fantástico do dia 05/11/2023 foi exibido um documentário da BBC, no qual é mostrado a luta da Parlamentar norte americana, Lauren Book, e da ativista britânica, Kate Isaacs, que foram vítimas do "pornô fake". Neste documentário, além de mostrar que qualquer pessoa pode ser vítima de *deepfakes*, mostrou que existe um mercado consumidor. Um dos "criadores" das *deepfakes*, o qual não foi identificado, relatou para BBC que a confecção de pornô fake é seu trabalho, que recebe USD$ 50,00 por minuto de vídeo e que as pessoas fazem encomendas não apenas de artistas, mas de pessoas próximas, como: mãe, irmã, colega de trabalho, amiga e vizinha. Não sendo pessoa famosa, tem que enviar uma foto ou um vídeo rápido das redes sociais desta e já será possível confeccionar um "pornô fake".

A fim de ilustrar essa questão de maneira mais concreta, podemos olhar outros dois exemplos que foram divulgados nas mídias e ocorreram no Brasil. Em Pernambuco, 40 adolescentes de um colégio particular de Recife foram vítimas de *deepfakes* produzidas e

compartilhadas pelos próprios alunos da escola[3], e o outro caso foi no Rio de Janeiro, onde 20 adolescentes foram vítimas do mesmo crime[4].

Apesar da legislação existente, como afirma Natuza Nery, presidente do Instituto Istart de ética digital, em entrevista ao portal G1, "você pode ter uma geração que queira fazer justiça com o próprio mouse, que não acredite nas instituições", além de pontuar a necessidade de investimento na educação digital preventiva em sala de aula. A criação e desenvolvimento de senso crítico e ético não só diminui o número de vítimas *online*, mas também o de criminosos.

CONCLUSÃO

A comunicação existe quando se tem a transmissão de uma mensagem, porém, pode ter o conteúdo que o remetente desejar, abrindo possibilidade para a inserção de inúmeros erros, informações falsas ou, pior, com intenção de prejudicar o destinatário. Na internet, faz-se saber, não só o destinatário terá acesso à mensagem, mas toda a sociedade virtual, que poderá, também, compartilhá-la com quem quiser.

É de se saber que crianças e adolescentes são seres humanos ainda em formação e plenamente incapazes de compreender completamente a realidade a seu redor, tornando-se o objeto de interesses maléficos de pessoas perversas num cenário tido como "sem leis".

Tratando sobre o principal crime que está crescendo nas redes sociais, o cyberbullying pela criação de imagens falsas, por meio da inteligência artificial, o presente trabalho se dedicou a pontuar as principais leis, como forma de atentar o leitor aos seus próprios direitos e deveres no âmbito digital, prosseguindo com a dissertação sobre os casos mais emblemáticos no Brasil e no mundo, como forma de destacar que o problema existe e as consequências não ficam "dentro das telas".

Por meio da pesquisa bibliográfica, este trabalho foi essencial para maior compreensão acerca do tema, porque entendemos que deve haver uma força tarefa para excomungar tais práticas do meio digital, preservando não só crianças e adolescentes, mas toda a sociedade. Tal força tarefa deve-se dar por ações do Estado, por meio de criação e aplicação de leis rígidas, além de educação digital às crianças e adolescentes, dos controladores de internet, por meio de

[3] Ler notícia na íntegra em <https://g1.globo.com/pe/pernambuco/noticia/2023/11/08/nudes-falsos-de-cerca-de-40-alunas-de-escola-do-recife-criados-por-colegas-mostravam-posicoes-pornograficas-e-foram-postados-em-redes-sociais-diz-pai.ghtml>.
[4] Ler notícia na íntegra em < https://g1.globo.com/podcast/o-assunto/noticia/2023/11/08/caso-de-nudes-falsos-acende-alerta-jovens-correm-risco-de-fazer-justica-com-um-mouse-diz-advogada.ghtml>.

tratamentos eficazes dos dados pessoais e sigilosos, das famílias, por meio da atenção às suas crianças e adolescentes, e das próprias pessoas, sendo possíveis vítimas, em prestarem atenção no que compartilham e acessam, sendo infratores, em não realizarem mais tais práticas e procurando ajuda especializada.

Como a abordagem do desenvolvimento deu-se sobre os princípios do direito penal brasileiro aplicáveis ao tema e a legislação pertinente, a ideia de se ter uma completa liberdade foi totalmente abolida, devendo ser compreendida como algo retrógrado e sem conexão com a atual conjuntura do país.

REFERÊNCIAS

BOND, Letycia. **Imagens de abuso sexual infantil online crescem em 70% no Brasil em 2023**. Agência Brasil, 2023. Disponível em: <https://agenciabrasil.ebc.com.br/geral/noticia/2023-05/imagens-de-abuso-sexual-infantil-online-crescem-70-no-Brasil-em-2023 >. Acesso em: 25 out. 2024.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 2023. Disponível em: <https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 21 out. 2024.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, DF: Presidência da República; 2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 21 out. 2024.

BRASIL. Ministério da Mulher, da Família e dos Direitos Humanos. **Lei nº 8.069, de 13 de julho de 1990**. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Diário Oficial da União, 1990. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/l8069.htm>. Acesso em: 21 out. 2024.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, 2014. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 21 out. 2024.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 21 out. 2024.

CARVALHO, Luann Motta. **BeReal possui polêmica política de coleta de dados dos usuários; entenda**. Olhar Digital, 2022. Disponível em: <https://olhardigital.com.br/2022/10/31/internet-e-redes-sociais/bereal-possui-polemica-politica-de-coleta-de-dados-dos-usuarios-entenda/>. Acesso em: 25 out. 2024.

CCJ do Senado aprova projeto para tornar hediondos crimes contra crianças e adolescentes. CartaCapital, 2023. Disponível em: <https://www.cartacapital.com.br/politica/ccj-do-senado-aprova-projeto-para-tornar-hediondos-crimes-contra-criancas-e-adolescentes/>. Acesso em: 25 out. 2024.

CURRY, David. **BeReal Revenue and Usage Statistics.** Business of Apps, 2023. Disponível em: <https://www.businessofapps.com/data/bereal-statistics/>. Acesso em: 25 out. 2024.

G1. **Ativista que luta contra pornografia criminosa também foi vítima de "pornô fake": "Querem me calar"**. Fantástico, 2023. Disponível em: <https://g1.globo.com/fantastico/noticia/2023/11/06/ativista-que-luta-contra-pornografia-criminosa-tambem-foi-vitima-de-porno-fake-querem-me-calar.ghtml>. Acesso em: 25 out. 2024.

G1. **Caso de nudes falsos acende alerta: "Jovens correm risco de fazer justiça com um mouse", diz advogada**. Rio de Janeiro, 2023. Disponível em: <https://g1.globo.com/podcast/o-assunto/noticia/2023/11/08/caso-de-nudes-falsos-acende-alerta-jovens-correm-risco-de-fazer-justica-com-um-mouse-diz-advogada.ghtml>. Acesso em 25 out. 2024.

G1. **"Nudes" falsos de cerca de 40 alunas criados por colegas de escola mostravam posições pornográficas e foram postados em redes sociais**. Pernambuco, 2023. Disponível em: <https://g1.globo.com/pe/pernambuco/noticia/2023/11/08/nudes-falsos-de-cerca-de-40-alunas-de-escola-do-recife-criados-por-colegas-mostravam-posicoes-pornograficas-e-foram-postados-em-redes-sociais-diz-pai.ghtml>. Acesso em: 25 out. 2024.

G1. **Sequestrador diz ter planejado crime com informações da rede social**. Santa Catarina, 2014. Disponível em: <https://g1.globo.com/sc/santa-catarina/noticia/2014/06/sequestrador-diz-ter-planejado-crime-com-informacoes-de-rede-social.html>. Acesso em: 25 out. 2024.

G1. **Viih Tube e Eliezer contam que pensaram em parar de postar fotos da filha de 7 meses após onda de xingamentos**. São Paulo, 2023. Disponível em: <https://g1.globo.com/fantastico/noticia/2023/11/19/viih-tube-e-eliezer-contam-que-pensaram-em-parar-de-postar-fotos-da-filha-de-7-meses-apos-onda-de-xingamentos.ghtml>. Acesso em: 25 out. 2024.

GABRIELE, Maiane. **O que é pedofilia virtual ou Ciberpedofilia?**. Quack redação, 2023. Disponível em: <https://quackredacao.com.br/o-que-e-pedofilia-virtual/>. Acesso em: 25 out. 2024.

GARCIA, Maria Carolina Brunharotto; NUNES, Paula Freire Santos Andrade. **Tratamento de dados pessoais de crianças e adolescentes: proteção e livre desenvolvimento do menor**

cercados pela LGPD e responsabilidade parental. 07 abr. 2021. Disponível em: <https://ibdfam.org.br/artigos/1673/Tratamento+de+dados+pessoais+de+crian%C3%A7as+e+adolescentes%3A+prote%C3%A7%C3%A3o+e+livre+desenvolvimento+do+menor+cercados+pela+LGPD+e+responsabilidade+parental>. Acesso em: 21 out. 2024.

GARRIDO, Patricia P. **Proteção de dados pessoais**: comentários à lei n. 13.709/2018 (LGPD). Editora Saraiva, 2023. E-book. ISBN 9786555599480. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786555599480/>. Acesso em: 21 out. 2024.

HENRIQUES, Isabella. Inteligência Artificial e publicidade dirigida a crianças e adolescentes. **Internet & Sociedade**, v. 2, n. 2, p. 5-25, 2021. Disponível em: < https://revista.internetlab.org.br/wp-content/uploads/2022/03/Inteligencia-artificial-e-publicidade-dirigida-a-criancas-e-adolescentes.pdf>. Acesso em: 25 out. 2024.

KOTSCHO, Mariana. **Uso da inteligência artificial por pedófilos aumenta a pornografia infantil na internet**. Uol, 2023. Disponível em: <https://marianakotscho.uol.com.br/criancas/uso-da-inteligencia-artificial-por-pedofilos-aumenta-a-pornografia-infantil-na-internet.html>. Acesso em: 25 out. 2024.

LAM, Lauro. **Crianças e adolescentes brasileiros são os que mais usam aparelhos eletrônicos no mundo, revela pesquisa da McAfee**. Olhar Digital, 2022. Disponível em: <https://olhardigital.com.br/2022/05/13/pro/criancas-e-adolescentes-brasileiros-sao-os-mais-conectados-do-mundo/>. Acesso em: 25 out. 2024.

MACHADO, Luciana Cristina Pinto; MARCONI, Licia Pimentel. **ESTUDOS PRELIMINARES SOBRE OS PRINCÍPIOS APLICADOS AO TRATAMENTO DE DADOS PESSOAIS NA LEI Nº 13.709/2018-LGPD**. Disponível em: <https://www.unoeste.br/Areas/Eventos/Content/documentos/EventosAnais/564/anais/Sociais%20Aplicadas/Direito.pdf#page=190>. Acesso em: 21 out. 2024.

MCGOWAN, Emma. **O BeReal tem boas intenções, mas e a privacidade?** Avast, 2022. Disponível em: <https://blog.avast.com/pt-br/bereal-safety>. Acesso em: 25 out. 2024.

NAZAR, Susanna. **Casos de pedofilia virtual se multiplicam com os avanços da inteligência artificial**. Jornal da USP, 2023. Disponível em: <https://jornal.usp.br/atualidades/casos-de-pedofilia-virtual-se-multiplicam-no-brasil-com-os-avancos-da-inteligencia-artificial/>. Acesso em: 25 out. 2024.

O que é GDPR e que diferença isso faz para quem é brasileiro. Tecnoblog, 2023. Disponível em: <https://tecnoblog.net/responde/gdpr-privacidade-protecao-dados/>. Acesso em: 21 out. 2024.

OLIVEIRA, Ingrid. **Criminosos usam "atalhos" nas redes para vender conteúdo de pedofilia**. Terra, 2023. Disponível em: <https://www.terra.com.br/byte/criminosos-usam-atalhos-nas-redes-para-vender-conteudo-de-pedofilia,f0e07800b8acf570e8aaadc56147be685nmyie3g.html>. Acesso em: 25 out. 2024.

RODRIGUES, Ana Julya da Costa; ARAÚJO, Débora Haquel Lima. **Crimes virtuais e seus reflexos na Legislação Brasileira**. 2023. Disponível em: <https://repositorio.animaeducacao.com.br/handle/ANIMA/34701>. Acesso em: 25 out. 2024.

SAFERNET. **Conheça a Lei para pornografia infantil**. Safernet, 2023. Disponível em: <https://new.safernet.org.br/content/conhe%C3%A7a-lei-para-pornografia-infantil>. Acesso em: 25 out. 2024.

SAFERNET. **Denúncias de imagem de abuso e exploração sexual infantil online tem aumento de 70% em 2023**. Safernet,2023. Disponível em: <https://new.safernet.org.br/content/denuncias-de-imagens-de-abuso-e-exploracao-sexual-infantil-online-compartilhadas-pela>. Acesso em: 25 out. 2024.

SAFERNET. **Safernet vence competição internacional e desenvolverá tecnologias de prevenção ao abuso sexual infantil**. Safernet, 2023. Disponível em: <https://new.safernet.org.br/content/safernet-vence-competicao-mundial-e-desenvolvera-tecnologias-de-prevencao-ao-abuso-sexual>. Acesso em: 25 out. 2024.