



PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
PRO-REITORIA DE GRADUAÇÃO
ESCOLA DE DIREITO, NEGÓCIOS E COMUNICAÇÃO
CURSO DE DIREITO
NÚCLEO DE PRÁTICA JURÍDICA
COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO

**DIREITO CONTEMPORÂNEO X INTELIGÊNCIA ARTIFICIAL
DESAFIOS, NORMAS E FISCALIZAÇÃO**

ORIENTANDO – DANIEL ALBERTO SENA ZENHA CARVALHO
ORIENTADORA- PROFA. TATIANA DE OLIVEIRA TAKEDA

GOIÂNIA-GO
2025

DANIEL ALBERTO SENA ZENHA CARVALHO

DIREITO CONTEMPORÂNEO X INTELIGÊNCIA ARTIFICIAL
DESAFIOS, NORMAS E FISCALIZAÇÃO

Artigo Científico apresentado à disciplina Trabalho de Curso II, da Escola de Direito, Negócios e Comunicação da Pontifícia Universidade Católica de Goiás.

Prof^a. Orientadora: MA. Tatiana de Oliveira Takeda.

GOIÂNIA-GO

2025

DANIEL ALBERTO SENA ZENHA CARVALHO

DIREITO CONTEMPORÂNEO X INTELIGÊNCIA ARTIFICIAL
DESAFIOS, NORMAS E FISCALIZAÇÃO

Data da Defesa: ____ de _____ de 2025.

BANCA EXAMINADORA

Orientadora: Prof^ª: MA. Tatiana de Oliveira Takeda

Nota

Examinadora Convidada: Profa.: Dra. Fernanda da Silva Borges

Nota

DIREITO CONTEMPORÂNEO X INTELIGÊNCIA ARTIFICIAL

DESAFIOS, NORMAS E FISCALIZAÇÃO

RESUMO

Daniel Alberto Sena Zenha Carvalho¹

A Inteligência Artificial tem se integrado de maneira cada vez mais intensa ao Direito contemporâneo, trazendo novas soluções para a gestão e o processamento de informações em diversas áreas. Embora existam ferramentas que auxiliem na elaboração de textos, em pesquisas na área da saúde, no compilamento de dados, entre outras, elas apresentam desafios quando se trata de segurança, controle e fiscalização. O Brasil conta com normas que buscam proteger o cidadão contra ataques virtuais, mas ainda carece de uma regulamentação específica sobre o uso da IA, especialmente no que diz respeito ao potencial de prejudicar, principalmente, os grupos mais vulneráveis. Essas preocupações evidenciam a necessidade de um controle e fiscalização que acompanhem o ritmo do avanço tecnológico, que é o foco deste estudo. A análise se baseou no método indutivo, com a observação de casos concretos para a construção das conclusões apresentadas, além de pesquisa bibliográfica que abordou normas, decisões judiciais e estudos essenciais para a compreensão do tema.

Palavras-Chave: Inteligência Artificial; Direito Contemporâneo; Desafios; Normas; Fiscalização.

CONTEMPORARY LAW VS. ARTIFICIAL INTELLIGENCE

CHALLENGES, REGULATIONS, AND OVERSIGHT

ABSTRACT

Artificial Intelligence has become increasingly integrated into contemporary Law, offering new solutions for the management and processing of information across various fields. While there are tools that assist in text drafting, health-related research, data compilation, among other applications, these technologies still face significant challenges regarding security, control, and oversight. In Brazil, there are legal norms aimed at protecting citizens against cyberattacks; however, the legal framework still lacks specific regulation concerning the use of Artificial Intelligence, particularly with respect to its potential to cause harm—especially to society’s most vulnerable groups. These concerns highlight the urgent need for a system of control and oversight that can keep pace with the rapid technological advancements, which is the central focus of this study. The analysis was conducted using the inductive method, based on the

¹ Daniel Alberto Sena Zenha Carvalho, Direito, 20192000101165@pucgo.edu.br

observation of concrete cases to support the conclusions presented herein. Additionally, a bibliographic review was carried out, covering legal norms, court decisions, and essential studies necessary for a comprehensive understanding of the topic.

Keywords: *Artificial Intelligence; Contemporary Law; Challenges; Standards; Inspection.*

SUMÁRIO

INTRODUÇÃO	4
1 A INTELIGÊNCIA ARTIFICIAL (IA)	6
1.1 CONCEITO.....	8
1.2 BREVE HISTÓRICO.....	9
1.3 CARACTERÍSTICAS.....	11
2 O DIREITO CONTEMPORÂNEO E SUAS IMPLICAÇÕES NO AMBIENTE VIRTUAL	13
2.1 AUSÊNCIA DE NORMAS ESPECÍFICAS PARA LIDAR COM A INTELIGÊNCIA ARTIFICIAL.....	14
2.2 A LEGISLAÇÃO CORRELATA.....	15
2.2.1 Lei nº 12.737/2012 (Lei Carolina Dieckmann).....	16
2.2.2 Lei nº 12.965/2014 (Marco Civil da Internet).....	18
2.2.3 Lei nº 13.709/2018 (Lei Geral de Proteção de Dados).....	19
2.2.4 Lei nº 14.155/2021.....	20
3 OS DESAFIOS DO DIREITO CONTEMPORÂNEO PARA LIDAR COM A INTELIGÊNCIA ARTIFICIAL E A NECESSIDADE DE CONTROLE E FISCALIZAÇÃO	20
3.1 DESAFIOS.....	20
3.1.1 Privacidade e Proteção de Dados.....	21
3.1.2 Propriedade Intelectual.....	22
3.1.3 Proteção do Público Vulnerável.....	23
3.2 CONTROLE E FISCALIZAÇÃO.....	24
CONCLUSÃO	28
REFERÊNCIAS	31

INTRODUÇÃO

A Inteligência Artificial (IA) tem provocado uma revolução em diversos setores sociais e o Direito não escapa dessa transformação. As tecnologias atuais de IA são moldadas ao aprendizado de redes neurais e algoritmos de predição que estão sendo gradativamente utilizados em processos judiciais e administrativos, prometendo maior eficiência, rapidez e acessibilidade. Desde a automação de tarefas repetitivas, como a análise de documentos e contratos, até a aplicação em sistemas de predição de resultados judiciais, a IA tem o potencial de mudar profundamente o funcionamento de todas as áreas.

Entretanto, a aplicação desta tecnologia no Direito também levanta uma série de questões e situações complexas. Entre seus maiores problemas é a imparcialidade de algoritmo, falta de segurança e restrição de dados frágeis. A IA, embora desenvolvida para ser objetiva e auxiliadora pode amplificar preconceitos presentes nos dados usados para treiná-la, como vieses raciais ou de gênero. Isso pode resultar em decisões discriminatórias ou injustas, algo particularmente problemático quando se trata de áreas sensíveis como o direito penal, onde as consequências das decisões podem ser graves. Os efeitos destes problemas inerentes à falta de fiscalização da IA, promove a ressonância de preconceitos e retrocessos sociais os quais o âmbito jurídico luta para extinguir.

Outro desafio relevante é a responsabilidade legal em casos onde a Inteligência Artificial toma decisões autônomas. Quando um sistema automatizado comete um erro, quem deve ser responsabilizado? O criador do algoritmo, o desenvolvedor do sistema, ou o usuário da ferramenta? Essa questão ainda carece estudos e questionamentos e muitos países já estão em processo de criação de regulamentações para lidar com essas questões.

Ademais, a utilização de IA também levanta preocupações com a privacidade e proteção de dados pessoais, em razão de grandes volumes de dados sensíveis, como por exemplo informações médicas ou bancárias. A maneira como esses dados são coletados, interpretados e armazenados precisa ser regulamentada de forma rigorosa para evitar abusos, vazamentos e outrora desinformação.

Do ponto de vista jurídico, um dos maiores desafios é a falta de uma legislação específica para regular a aplicação da Inteligência Artificial no Direito. As normas

existentes muitas vezes não abordam de forma adequada os avanços tecnológicos rápidos, criando um vácuo jurídico que dificulta a supervisão e o controle. Embora alguns países estejam começando a implementar regulamentos para proteger a privacidade e garantir a transparência no uso desta tecnologia, a legislação global ainda está em desenvolvimento.

O método empreendido será o indutivo, em razão das observações de casos da realidade concreta, o que enseja constatações particulares. O tipo de pesquisa a ser empregada será a bibliográfica, limitada aos objetivos, problemas e hipóteses levantadas. A pesquisa bibliográfica, do ponto de vista do procedimento técnico, é fundamental, considerando que fornece um estudo teórico, embasado em normas, julgados e doutrinas.

A implementação da Inteligência Artificial necessita de abordagem que disponha sobre controle e fiscalização e para direcionar o presente estudo as seções irão explicar de forma didática o que é, o que faz, como é tratada no ordenamento jurídico, o que falta e o que e como pode ser feito

Assim, a Seção 1 abordará a criação da Inteligência Artificial, em termos históricos a seus desenvolvedores e criadores.

Por sua vez, a Seção 2 disporá sobre a legislação correlata em relação a IA e as normas legislativas vigentes no cenário brasileiro que se relacionam com a tecnologia.

Por fim, a Seção 3 mostrará os desafios a frente a grupos e espectros sujeitos aos riscos da Inteligência Artificial expondo a vulnerabilidade com a qual a IA se infiltra.

1. A INTELIGÊNCIA ARTIFICIAL (IA)

1.1. CONCEITO

A Inteligência Artificial (IA) é oriunda do campo de estudo tecnológico que simula a reprodução de habilidades humanas, produzindo raciocínios, dados, elementos de aprendizagem e criatividade a partir de um banco de dados fornecido previamente que compõe diversas formas combinatórias desses dados em infinitas possibilidades de resultados. Sendo assim, essa reprodução do intelecto humano

possibilita a sistematização e automatiza tarefas intelectuais e, portanto, é potencialmente elegível para ser indispensável para qualquer esfera da atividade intelectual humana.” Nesse sentido, ela é um campo universal”(Russell; Norvig, 2004).

Haugeland (1985, p. 235) enxerga essa habilidade pensativa análoga à forma humana ao dispor que “o novo e interessante esforço para fazer os computadores pensarem... máquinas com mentes, no sentido total e literal. Dessa forma, fica explícito o cerne intelectual autônomo e independente, de forma análoga a forma autônoma que a mente humana possui.

Ao utilizar processos cognitivos e padrões comportamentais, a IA consegue simular atividades mentais, tornando-se uma tecnologia cada vez mais independente e com potencial de eficiência enorme que se assemelha quase que imperceptível e paralelamente às atividades humanas.

1.2 BREVE HISTÓRICO

É possível descrever a origem da Inteligência Artificial a partir dos anos 40 do século XX, quando cientistas de diversas áreas compreendendo desde a psicologia à robótica e célebres da informática uniram conhecimentos até então para reproduzirem comportamentos humanos em máquinas inteligentes e autônomas a partir de dados programados. Acerca dessa comparação entre homem e máquina, Gomes (2010, p. 236) expõe:

Pode-se dizer que o primeiro grande trabalho reconhecido como IA foi realizado por Warren Macculloch e Walter Pitts (1943). De acordo com Russell e Norvig (2004), eles se basearam em três fontes: “o conhecimento da fisiologia básica e da função dos neurônios do cérebro, uma análise formal da lógica proposicional criada por Russell e Whitehead e a teoria da computação de Turing”. Esses pesquisadores sugeriram um modelo de neurônios artificiais, no qual, cada neurônio era caracterizado por “ligado” ou “desligado”, desse modo, o estado de um neurônio era analisado como, “equivalente em termos concretos a uma proposição que definia seu estímulo adequado”.

Os programadores Warren McCulloch, Walter Pitts e Allan Turing foram os precursores do desenvolvimento desta tecnologia que veio a público apenas em 1956, por John McCarthy (Zendesk, 2024). Além disso, Gomes (2010) explica:

Contudo, foi Alan Turing o primeiro a articular uma visão completa da IA em seu artigo de 1950 “Computing Machinery and Intelligency”. Ele apresentou o

Teste de Turing, onde sugeriu um teste baseado na impossibilidade de distinguir entre entidades inegavelmente inteligentes, “os seres humanos”. O computador passará no teste se um interrogador humano, depois de propor algumas perguntas por escrito, não conseguir descobrir se as respostas escritas vêm de uma pessoa ou não.

A crescente e gradativa atração desses estudiosos na década 50 é disseminada nas mais consagradas universidades do mundo em congressos ou eventos voltados para essa área que ao longo dos anos receberam investimentos em estudos internos cada vez mais elaborados, de qualidade e de consequente sucesso. Nos vinte anos seguintes, o campo seria dominado por essas pessoas e por seus alunos e colegas do MIT, da CMU, de Stanford e da IBM (Russell; Norvig, 2004).

Diversos países, entre ocidente e oriente implementavam desenvolvimentos para a IA proeminentes devido à alta capacidade e diversas atuações que esta tecnologia poderia inferir nos processos, atividades e cotidiano humanos. Essa busca por progresso para a Inteligência Artificial incitou atritos competitivos entre diversos países acelerando estudos e realizando “contragolpes” em contrapartida a cada avanço executado por cada país, universidade ou continente. Em relação a essa competitividade, Gomes (2010) exemplifica:

Em 1981, os japoneses anunciaram o projeto Fifth Generation, um plano de 10 anos para montar computadores inteligentes por meio da utilização do Prolog. Em Resposta, os Estados Unidos constituíram a Microelectronics and Computer Technology Corporation (MCC) como um consórcio de pesquisa projetado para assegurar a competitividade nacional. Em ambos os casos, a IA fazia parte de um amplo esforço, incluindo o projeto de chips e a pesquisa da interface humana.

Posteriormente, em Stanford, Estados Unidos, surge o primeiro protótipo tecnológico com resultados concretos e eficientes. Isso se comprova na participação do Dendral de forma similar à autonomia intelectual humana, sendo capaz de gerar resultados que os próprios pesquisadores não conseguiram determinar. De acordo com Gomes (2010, p. 239):

Em 1969, a Universidade de Stanford desenvolveu o programa DENDRAL para desenvolver soluções capazes de encontrar as estruturas moleculares orgânicas a partir da espectrometria de massa das ligações químicas presentes em uma molécula desconhecida. Na época, personagens importantes como Edward Feigenbaum (antigo aluno de Herbert Simon), Bruce Buchanan (filósofo transformado em cientista de computação) e Joshua Lederberg (geneticista premiado com um prêmio Nobel) constituíram equipe para resolver o problema e o DENDRAL foi capaz de solucionar graças ao seu modo automático de tomar decisões.

A partir de 1980, a tecnologia da IA sofre o processo de industrialização e passa a ser produto de comercialização nas diversas áreas humanas por diversas empresas já proporcionando lucros extremamente notáveis no setor. Essa industrialização é vista em programas de execução intermediando solicitações de clientes da área da informática com o produto adequado, a exemplo o DEC, que em seu auge, no ano de 1988 era responsável por retorno lucrativo interessante, como dispõe Gomes (2010) ao apontar que “o programa contribuiu para configurar pedidos de novos sistemas de computador; em 1986, ele já fazia a empresa faturar cerca de 40 milhões de dólares por ano”.

Com esse crescimento da IA como mão de obra no mercado de trabalho a partir da década de 80, suas atuações passam a servir diversas áreas acadêmicas, sociais e laborais.

Além disso, nessa mesma época, ocorre a diversificação e ramificação de sistemas, dando-se atenção à agricultura, química, sistemas de computadores, eletrônica, engenharia, geologia, gerenciamento de informações, direito, matemática, medicina, aplicações militares, física, controle de processos e tecnologia espacial. Para Gomes (2010, p. 239):

A partir dessa época, vários sistemas foram desenvolvidos para atuação em diferentes domínios, como por exemplo, agricultura, química, sistemas de computadores, eletrônica, engenharia, geologia, gerenciamento de informações, direito, matemática, medicina, aplicações militares, física, controle de processos e tecnologia espacial.

É interessante citar um feito da IA em 1991, nos ápices dos eventos da Guerra do Golfo, conflito bélico liderada pelos Estados Unidos contra o Iraque, um espécime da Inteligência Artificial, denominado “Dart”, com a função de criar estratégias nas performances de deslocamento dos soldados em terras iraquianas, foi largamente utilizada diretamente pelos soldados americanos, que segundo as agências militares, foram responsáveis por grande êxito das atividades ali executados pelos próprio americanos (Gomes, 2010).

A IA deixou de ser apenas matéria de trabalho acadêmico ao provar sua habilidade em campo de forma literal. Contemporaneamente, sua consolidação nos campos de pesquisa e estudo são intensificados para que sejam propagados não

somente em situações específicas ou eventuais, como na guerra descrita, mas sim no cotidiano ordinário que se vivencia.

1.3 CARACTERÍSTICAS

A autonomia da Inteligência Artificial pode ser descrita como a capacidade de simular a inteligência humana, produzindo raciocínios complexos e extremamente semelhantes realizando tarefas e execuções complexas de forma natural e imperceptível ao próprio olho humano.

Deve-se destacar a produção de resultados probatórios a partir deste banco de dados promovendo análises cada vez mais embasadas no coeficiente final do objeto estudado. Esta análise serve como uma previsão que busca evitar erros a partir dos fatores e fatos ocorridos influenciando resultados mais firmes e analíticos.

Distribui-se a Inteligência Artificial em alguns eixos para que seja executada: um banco de dados referentes como base para a análise, desde que estes dados não estejam processados possibilitando a imprevisibilidade e criação dos resultados e a classificação de *inputs* que são dados pré-estabelecidos de entrada que gera e distribui os demais conteúdos na máquina (Morais; Branco, 2023, p. 1).

Para a execução da Inteligência Artificial, existem usos específicos e destinos para as demais atividades. Sendo assim, se dividem em três categorias, como aponta Moraes e Branco (2023, p. 05):

Inteligência de Máquina: Esta inteligência tem o objetivo de criar máquinas capazes de realizar tarefas específicas programadas, por exemplo, reconhecer padrões, tomar decisões lógicas ou aprender a partir de experiências anteriores e, sua aplicação tem como objetivo automatizar processos e simplificar tarefas diárias. **Inteligência Humanoide:** Esta inteligência visa criar máquinas capazes de imitar o comportamento humano. Essas máquinas são programadas para se comportar de forma semelhante aos seres humanos, realizando tarefas como conversar, reconhecer faces ou expressar emoções. Sua aplicação tem a ver com a criação de interfaces digitais mais humanizadas e inteligentes em dispositivos. **Inteligência Coletiva:** Esta inteligência busca desenvolver redes complexas capazes de tomar decisões coletivas. Essas redes são formadas por múltiplos agentes inteligentes interconectados, que trabalham juntos para solucionar problemas. O intuito é criar sistemas complexos capazes de tomar decisões coletivas, como um sistema financeiro inteligente. (grifo original)

É relevante ressaltar a importância da interação entre humanos e máquinas, garantindo que as tarefas realizadas estejam alinhadas aos propósitos previamente

definidos. Para que essa interação ocorra de forma eficiente e compreensível, destaca-se o papel fundamental do Processamento de Linguagem Natural (PLN), cuja principal finalidade é criar tecnologias que possibilitem uma comunicação clara e objetiva entre pessoas e sistemas computacionais. Isto se comprova em chats, pesquisas, atendimentos on-lines, etc. Em relação a este processo, Moraes e Branco (2023, p. 7) dispõem que “o processamento de linguagem natural consiste na utilização da tecnologia de *machine learning*, permitindo que o sistema analise, entenda, encontre padrões, insights e, seja capaz de gerar a linguagem humana escrita e falada de modo natural”.

Sendo assim, o processo de linguagem natural é imprescindível para a confecção da relação linguística entre homem e máquina proporcionando a compreensão automática da própria Inteligência Artificial dinamizando as operações e enriquecendo as diversas possibilidades de análises, padrões, dados e transformando em conhecimento cada vez mais complexo e aprofundado.

2. O DIREITO CONTEMPORÂNEO E SUAS IMPLICAÇÕES NO AMBIENTE VIRTUAL

2.1. AUSÊNCIA DE NORMAS ESPECÍFICAS PARA LIDAR COM A INTELIGÊNCIA ARTIFICIAL

A ausência de normas específicas para regulamentar a Inteligência Artificial configura um dos maiores impasses jurídicos e éticos da contemporaneidade. Em um cenário de progresso acelerado dessa tecnologia, a lacuna normativa se apresenta como um desafio multifacetado, que compromete a segurança, a justiça e a proteção dos direitos individuais. A falta de uma estrutura legal precisa sobre o uso desta tecnologia resulta em uma crescente e gradativa insegurança acerca de questões cruciais, como a responsabilidade por decisões automatizadas, a imparcialidade dos algoritmos e a privacidade dos dados pessoais. Este vazio normativo não apenas expõe vulnerabilidades no sistema jurídico, mas também abre brechas para abusos e práticas empresariais que podem explorar os cidadãos de maneira nociva.

A inexistência de regras claras e restritas facilita o uso indiscriminado de suas aplicações, sem a devida supervisão, regulando apenas de forma difusa aspectos periféricos da tecnologia. O risco de discriminação dos algoritmos, violação de direitos humanos e manipulação de processos decisórios, sem a devida responsabilidade, coloca em xeque a própria confiança nas instituições. Diante desse cenário de incertezas, impõe-se a urgência de uma legislação robusta e adaptativa, que, ao mesmo tempo em que fomente o avanço tecnológico, assegure os direitos fundamentais dos indivíduos e promova a transparência, a ética e a equidade no uso da IA. A falta de uma regulação eficaz agrava a instabilidade, exigindo uma resposta legislativa que consiga balancear inovação com responsabilidade.

2.2. LEGISLAÇÃO CORRELATA

Embora o Brasil tenha avançado com marcos regulatórios como o Marco Civil da Internet e a Lei Geral de Proteção de Dados (LGPD), estes dispositivos ainda são insuficientes para lidar com os desafios e as questões éticas que surgem com o uso de Inteligência Artificial.

A ausência de uma legislação clara e específica coloca em risco direitos fundamentais como a privacidade, a liberdade de expressão e o direito à não discriminação. Além disso, sem regulamentação própria, torna-se difícil garantir a transparência nos algoritmos e a responsabilização de quem usa essas tecnologias.

O atraso na criação de normas específicas para a regulação da Inteligência Artificial no Brasil é um reflexo da rapidez com que as tecnologias evoluem, superando o ritmo da legislação.

A falta de um marco regulatório robusto impede que as leis existentes, como o Marco Civil, possam ser aplicadas de forma eficaz em relação às questões contemporâneas da Inteligência Artificial. Isso cria um vácuo jurídico onde a utilização de algoritmos e sistemas inteligentes podem ocorrer de maneira desregulada, o que representa riscos significativos para a sociedade.

A regulamentação específica seria essencial para assegurar que a inovação tecnológica aconteça de forma ética e que a sociedade possa se beneficiar da Inteligência Artificial sem comprometer direitos fundamentais.

Além disso, o marco regulatório para a IA também precisa tratar da questão da responsabilidade. Com a utilização crescente de sistemas autônomos, como

veículos autônomos ou algoritmos de decisões judiciais, surge a dúvida sobre quem será responsabilizado caso algo dê errado. A falta de clareza jurídica em relação à responsabilização por danos causados por IA ou por decisões automatizadas pode resultar em impunidade ou em vítimas desprotegidas. Portanto, uma legislação que contemple esses aspectos seria essencial para evitar que os avanços tecnológicos comprometam a justiça e a equidade social.

A regulamentação, portanto, é uma questão de justiça e ideologia de segurança social, pois ao criar uma legislação específica, o Brasil poderia estabelecer um sistema que equilibrasse a inovação tecnológica com os direitos dos cidadãos. Isso incluiria não apenas a proteção contra o uso indevido de dados, mas também o monitoramento da aplicação de IA de forma a evitar discriminação e viés algorítmico.

2.2.1 Lei nº 12.737/2012 (Lei Carolina Dieckmann)

A Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, é um marco no enfrentamento de crimes cibernéticos no Brasil, especialmente aqueles relacionados à invasão de dispositivos eletrônicos e à violação da privacidade de indivíduos. Ela estabelece punições para quem acessa dispositivos de terceiros, como computadores e celulares, sem autorização, visando proteger a integridade e a privacidade das informações pessoais armazenadas nessas tecnologias. Ademais, é interessante a relevância social que o caso tomou devido à influência social da atriz.

A relação dessa lei com a Inteligência Artificial é, de certa forma, indireta, mas significativa no contexto do desenvolvimento e uso de tecnologias avançadas. A IA pode ser tanto um instrumento para a violação das normas previstas na Lei Carolina Dieckmann quanto uma aliada na identificação e prevenção desses crimes.

O avanço indiscriminado da IA, por meio de técnicas como o aprendizado de máquina, pode ser utilizado por criminosos para facilitar invasões e acessos não autorizados a dispositivos, aumentando a complexidade dos delitos cibernéticos. Por exemplo, algoritmos que podem ser empregados para a criação de malwares mais sofisticados ou ataques de phishing mais direcionados, aproveitando-se das vulnerabilidades digitais para acessar informações pessoais de maneira furtiva e eficiente.

Por outro lado, a IA também pode ser um recurso valioso na identificação de crimes cibernéticos. Tal valor se deve à capacidade de detectar padrões de

comportamentos suspeitos, automatizar a análise de grandes volumes de dados e identificar tentativas de invasão de dispositivos, ajudando na investigação e no combate à violação de dispositivos eletrônicos. Ferramentas baseadas em IA podem auxiliar, por exemplo, em programas de monitoramento e prevenção de ataques cibernéticos, detectando anomalias no tráfego de dados e alertando para possíveis invasões.

Em síntese, a Lei nº 12.737/2012 tem uma relação com a IA tanto no aspecto de proteção, como também no de ameaça, pois esta pode ser empregada para facilitar crimes digitais ou para fortalecer os mecanismos de combate a esses crimes. A legislação precisa evoluir continuamente para acompanhar as mudanças tecnológicas e garantir que as inovações não sejam usadas de maneira indevida.

2.2.2 Lei nº 12.965/2014 (Marco Civil da Internet)

A Lei nº 12.965/2014, conhecida como Marco Civil da Internet, estabelece os direitos e deveres dos usuários e provedores de serviços na rede, com o objetivo de garantir a cidadania digital e a proteção dos dados pessoais.

No contexto da Inteligência Artificial, essa legislação adquire relevância ao estabelecer parâmetros e princípios fundamentais como a liberdade de expressão, a privacidade e a proteção de dados. A IA, ao processar grandes volumes de informações, pode tanto se relacionar com as delimitações impostas pelas normas do Marco Civil, especialmente no que se refere ao tratamento e armazenamento de dados pessoais dos usuários, garantindo que esses processos ocorram de forma ética e legal. Para Carvalho (2017, p. 231) “o Marco Civil da internet trouxe, em artigos diferenciados, a regulamentação da responsabilidade de cada um dos tipos de provedores”.

A privacidade é um dos pilares do Marco Civil da Internet e a IA tem um impacto direto sobre isso, já que sistemas de aprendizado de máquina frequentemente coletam e analisam dados pessoais para fornecer soluções personalizadas. Nesse sentido, o artigo 7º da Lei nº 12.965/2014, que trata da proteção de dados, exige que as plataformas sigam normas rigorosas para garantir que os dados dos usuários sejam utilizados de forma segura e transparente.

O Marco Civil da Internet define a responsabilidade dos provedores de internet quanto ao conteúdo gerado por terceiros. A tecnologia ao interagir com grandes

volumes de dados e gerar conteúdos, como textos, imagens ou até decisões automatizadas, levanta questões sobre quem é responsável por suas ações e suas consequentes intenções.

Se uma plataforma de gerar conteúdos difamatórios ou prejudiciais, a questão da responsabilidade legal deve ser cuidadosamente analisada, já que os sistemas podem ser projetados para agir de maneira autônoma, sem supervisão direta, assim como a plataforma gerar danos em determinadas áreas visíveis e existentes no campo jurídico. Acerca desta autonomia dos sistemas, o Marco Civil altera e dispensa a culpabilidade dos sistemas e plataformas os responsabilizando provocando a busca por meios seguros de proteção de dados. Acerca dessa alteração e consequente responsabilização, Carvalho (2017, p. 232) dispõe que:

Com a nova regulamentação é afastada a responsabilidade irrestrita dos provedores de aplicações, considerando que eles só serão responsabilizados se não cumprirem a condição determinada pela lei, qual seja, retirar da web o conteúdo ilícito gerado por terceiros após ordem judicial específica. Nesse ponto, buscou o legislador elevar o direito fundamental à liberdade de expressão, considerando que não será retirado o conteúdo veiculado pela simples denúncia ao provedor, sendo necessária ordem judicial específica, sem a qual não poderá ser indisponibilizado qualquer conteúdo em prol de usuários que se sintam lesados com determinada publicação, salvo disposições legais em contrário. Ademais, além da obrigatoriedade de cumprir a ordem judicial, a fim de se resguardar de qualquer responsabilidade, os provedores de aplicações deverão prestar todas as informações necessárias para identificação dos usuários transgressores, sendo que os registros de acesso a aplicações de internet deverão ser guardados sob sigilo pelo prazo de seis meses, sob pena de responderem civilmente pelas perdas e danos causados, conforme o artigo 15 da lei em comento. Assim, verifica-se que a responsabilidade dos provedores de aplicações só será do tipo objetiva⁷ quando o ato ilícito se originar do próprio provedor, sendo necessário à vítima provar, tão somente, a autoria e o dano para obter êxito na ação reparatória

Por fim, a inclusão digital é outro ponto crucial que conecta o Marco Civil da Internet e a IA. O Marco Civil propõe que todos os cidadãos tenham acesso à internet de forma equitativa, o que pode ser impactado pela IA. Tecnologias baseadas em IA podem contribuir para a inclusão, oferecendo soluções personalizadas e acessíveis, mas também podem ampliar a exclusão digital se não forem adequadamente reguladas. Portanto, é essencial que as políticas públicas e a regulamentação do uso da IA promovam a inclusão digital, de forma que todos os usuários tenham acesso aos benefícios das tecnologias sem serem prejudicados por um mercado digital desigual.

2.2.3 Lei nº 13.709/2018 (Lei Geral de Proteção de Dados)

A Lei nº 13.709/2018, também conhecida como Lei Geral de Proteção de Dados (LGPD), estabelece diretrizes para o tratamento de dados pessoais no Brasil, com o objetivo de garantir a privacidade e a segurança dos dados dos cidadãos.

A relação entre a LGPD e a IA é direta, pois a esta depende do processamento de grandes volumes de dados, muitas vezes pessoais, para gerar seus resultados. Assim, a implementação de sistemas de IA precisa respeitar os princípios da LGPD, garantindo que o tratamento de dados seja feito de forma transparente, lícita e segura.

A coleta e o uso de dados pessoais por sistemas de IA devem estar em conformidade com os direitos dos titulares previstos pela LGPD. A lei exige que o consentimento seja obtido de maneira clara e explícita, permitindo que os indivíduos saibam como seus dados serão utilizados. No contexto da IA, isso significa que os usuários precisam ser informados sobre o tipo de dados que estão sendo coletados, a finalidade do uso e os possíveis impactos desse tratamento. Além disso, a possibilidade de revogar o consentimento é um direito essencial para garantir a autonomia dos titulares.

Outro ponto crucial da LGPD em relação à IA é a segurança dos dados. A lei impõe que as empresas adotem medidas técnicas e administrativas para proteger os dados pessoais contra acessos não autorizados, vazamentos ou outras formas de tratamento indevido.

Os sistemas de IA, por sua natureza, lidam com grandes quantidades de dados, o que torna ainda mais importante a implementação de salvaguardas eficazes. No contexto jurídico, ela assegura a privacidade dos cidadãos, impondo responsabilidades a advogados, empresas e órgãos públicos que lidam com informações sensíveis. Essa legislação fortalece os direitos dos indivíduos, ao mesmo tempo em que orienta as práticas de conformidade e governança de dados no setor. Por oportuno, cita-se Silva, Souza e Silva (2024):

O uso da IA impacta na Lei Geral de Proteção de Dados, mormente quando o treinamento algoritmo viabiliza a utilização de dados pessoais. Isto se justifica pela necessidade da tecnologia de construir seu método a partir de cruzamento de dados, conforme demonstrado anteriormente. Quanto maior o número de dados, maior será a qualidade da IA. Entrementes, a preocupação é majorada ao discutir este cenário no âmbito jurídico, quando da coleta de dados pessoais e impactos do uso de ferramentas tecnológicas.

A Lei n. 13.709/2018, no inciso VII do art. 2º, dispõe os direitos humanos e o exercício da cidade como fundamento perante os critérios da LGPD, diploma sob a influência do Regulamento Geral de Proteção de Dados da União Europeia.

Diante disso, há dois contextos a serem analisados: o primeiro, sob o ponto de vista da advocacia, a virtualização dos atos processuais proporcionou benefícios e obstáculos, quanto a este último, envolve a atividade jurisdicional e o segundo contexto, o Judiciário. Que a inteligência artificial atinge a atividade judicante não é novidade, principalmente os atos de expediente, de admissibilidade recursal ou seleção de temáticas a serem submetidas às Cortes Superiores, estas já integrantes na realidade do sistema judiciário brasileiro. O foco gira em torno da atividade-fim, aquela exercida pela Jurisdição, em sua função de julgar os casos.

Portanto, para o setor jurídico, a conformidade com a LGPD não deve se tratar apenas uma obrigação ou mero dispositivo legal de fiscalização mas uma oportunidade de fortalecer a confiança e a transparência nas relações entre profissionais, clientes e instituições. Assim, a legislação se torna essencial para promover um ambiente mais seguro e ético na gestão de dados dentro do campo jurídico.

2.2.4 Lei nº 14.155/2021

A Lei nº 14.155/2021, que alterou o Código Penal Brasileiro, introduziu mudanças significativas no tratamento de crimes cometidos por meio de meios eletrônicos, como o uso de sistemas de Inteligência Artificial.

A nova legislação, ao agravar as punições para fraudes digitais e crimes cibernéticos, reflete a crescente preocupação com os riscos associados ao uso de tecnologias e a prevenção de crimes eletrônicos.

A implementação de controles eficazes de segurança pode contribuir para reduzir a vulnerabilidade a crimes digitais, protegendo usuários e sistemas. A automatização de processos por sistemas de Inteligência Artificial pode ser explorada para a realização de crimes, como fraudes, fraudes bancárias e crimes de dados, o que exige uma regulamentação mais robusta para combater esses delitos. Por oportuno, cita-se Figueiredo (2021, p.14):

Uma das alterações promovidas pela Lei 14.155 de 2021 ocorreu no crime de invasão de dispositivo informático, previsto no art. 154-A do Código Penal. 2.1. Alteração no tipo simples e na cláusula de equiparação O art. 154-A, caput do Código Penal foi criado, originariamente, pela Lei 12.737 de 2012, a qual ficou conhecida como Lei Carolina Dieckmann. Com efeito, naquele ano, a famosa atriz teve dispositivo pessoal invadido e, na sequência, foram

divulgadas fotos íntimas suas, as quais constavam no aparelho. O caso teve bastante repercussão e, em razão disso, o legislador pátrio agiu para criar um tipo penal que criminalizasse tal tipo de comportamento. Desta feita, o legislador modificou o tipo incriminador e, também, previu maior sancionamento para o comportamento.

A relação entre a Lei nº 14.155/2021 e a IA é evidenciada na necessidade de responsabilização de quem utiliza sistemas automatizados para a prática de ilícitos. A utilização de IA para cometer crimes, como fraudes financeiras ou falsificação de documentos, por exemplo, pode ser dificultada pela falta de uma regulamentação clara sobre a responsabilidade dos agentes que operam tais sistemas.

A lei estabelece que por se tratar de fraudes digitais, as punições podem ser mais severas, reforçando a necessidade de uma vigilância constante sobre as ações de IA em ambientes virtuais. Dessa forma fica evidente a relação do campo tecnológico com os diversos crimes que diversos e hediondos que surgem com o advento da IA. Sobre esta correlação a abertura de crimes para serem vistos de forma integral, tomando como base no caso da atriz Dieckmann:

Por fim, a interação entre a IA e a Lei nº 14.155/2021 evidencia a importância de uma abordagem ética no desenvolvimento de tecnologias. A lei busca não apenas punir os crimes cometidos, mas também incentivar práticas responsáveis por parte dos desenvolvedores desta tecnologia, a fim de garantir que a tecnologia seja usada para o benefício da sociedade e não para a realização de atos ilícitos.

3. OS DESAFIOS DO DIREITO CONTEMPORÂNEO PARA LIDAR COM A INTELIGÊNCIA ARTIFICIAL E A NECESSIDADE DE CONTROLE E FISCALIZAÇÃO

3.1. DESAFIOS

A Inteligência Artificial promove vários desafios e questões intrínsecas, devido ao manejo com que os dados são expostos e utilizados por ela. A autonomia desenfreada de IA pode perpetuar e transmitir discriminação quando assimilada com algoritmos e dados que propagam teores criminosos, vexatórios e socialmente difamatórios.

Além disso, ocorre que a transparência nos algoritmos dificulta a compreensão de como as decisões são tomadas, gerando até mesmo desconfiança.

Deve-se reiterar que essa preocupação com a segurança privada de dados em relação a IA vem sendo agravada pelo próprio público comum devido à autonomia dos dados com os quais a IA se abastece, já que sistemas podem ser alvo de ataques cibernéticos, comprometendo dados sensíveis e vulneráveis de ordem pessoal e intelectual. Esse mesmo público já encontra deformidades, brechas visíveis que são possíveis riscos à integridade pessoal. Tendo em vista esta insegurança, nos apontam Sampaio, Sabbatini e Limongi (2024, pág. 16):

Apesar dos benefícios observados, houve uma desconfiança em relação às empresas de IAG, com apenas 8% dos participantes confiando que essas empresas não usariam seus dados sem permissão. Além disso, 59% dos respondentes acreditam que a IA pode enfraquecer a propriedade intelectual, e 25% acham que reduz a necessidade de pensamento crítico, refletindo preocupações profundas sobre o impacto da tecnologia no rigor acadêmico.

Outro desafio é a responsabilidade legal, já que é difícil identificar quem deve ser responsabilizado por erros cometidos por sistemas autônomos.

No campo jurídico, área que a ética e o comportamento são estruturas norteadoras desta profissão, é extremamente explícita a necessidade por um controle fiscalizador para que não contrarie os princípios básicos jurídicos. Acerca disto, ensinam Silva, Souza e Silva (2024):

Dentro do contexto jurídico existem algumas maneiras, tais como o viés nos dados (Os algoritmos de IA são frequentemente treinados com conjuntos de dados históricos que refletem preconceitos sociais existentes. Se esses dados históricos contiverem viés racial, de gênero, socioeconômico ou outro tipo de preconceito, os algoritmos podem reproduzir e até amplificar esses vieses em suas decisões), viés na programação (Os próprios programadores podem inadvertidamente introduzir viés em algoritmos por meio de escolhas de design ou decisões de codificação. Por exemplo, decisões sobre quais recursos incluir ou excluir em um algoritmo podem influenciar fortemente os resultados e potencialmente introduzir viés.), falta de transparência (muitos sistemas de IA utilizados no Direito são “caixas-pretas”, o que significa que seus processos de tomada de decisão são obscuros e não facilmente compreensíveis pelos usuários finais. Isso dificulta a identificação e a correção de qualquer viés algorítmico presente nos sistemas.), reforço de preconceitos existentes (algoritmos de IA podem inadvertidamente perpetuar preconceitos ao longo do tempo, à medida que aprendem com os dados de entrada e interações com o ambiente. Isso pode levar a um ciclo de reforço, onde decisões preconceituosas do passado são usadas para informar decisões futuras, perpetuando assim o viés.), entre outros que estimulam e levam ao pensamento ético e jurídico de como essa ferramenta (IA) vem se destacando e gerando desafios dentro do contexto legal.

Sendo assim, fica visível que por mais seja uma ferramenta extremamente inteligente e pareça ser a frente do seu tempo, a IA bebe da própria história humana, juntamente com suas doenças, preconceitos, atos hediondos e fatos tenebrosos. A discricionariedade com que trabalha a IA é um motivo de alerta para que todos esses temas, que embora mesmo no presente ainda-se refutam, o retrocesso não ocorra ao manejo errado desta ferramenta e fujam do compromisso que a ética trabalha diariamente.

3.1.1. Privacidade e proteção de dados

A privacidade e a proteção de dados são direitos fundamentais que garantem a segurança das informações pessoais dos indivíduos em redes virtuais. Com o avanço gradativo e irremediável da tecnologia e o uso crescente da internet em todo o globo a coleta e o processamento de dados tornaram-se práticas comuns, o que levanta preocupações sobre o uso indevido dessas informações.

Devido a transição da exposição social para as redes sociais que estão a um toque, a periculosidade dos dados pessoais sofre aumento à suscetibilidade de vulnerabilidade e consequentes vazamentos. Acerca deste tema, Domingues e Silva (2024, p.162) explicam que:

A privacidade é um direito fundamental expressamente protegido por diversas legislações ao redor do mundo, incluindo a Constituição Federal Brasileira. Em um mundo cada vez mais digitalizado, onde informações pessoais são constantemente coletadas, processadas e armazenadas por sistemas de IA, a necessidade de proteger esses dados torna-se imperativa. A proteção de dados pessoais não apenas resguarda a privacidade individual, mas também fortalece a confiança na forma como as instituições gerenciam as informações.

A proteção de dados visa evitar vazamentos, acessos não autorizados e abusos, enquanto a privacidade assegura que o indivíduo tenha controle sobre suas informações pessoais. As normas como a Lei Geral de Proteção de Dados (LGPD) surgem para regulamentar e assegurar esses direitos, estabelecendo obrigações para empresas e organizações que lidam com dados pessoais. A implementação de medidas adequadas de segurança é essencial para proteger a privacidade dos usuários em um cenário cada vez mais digitalizado.

Além de ser uma questão ética, a proteção de dados também se configura como uma necessidade estratégica para empresas e governos. De acordo com Silva e Domingues (2024, p. 163), as “organizações que demonstram habilidade em proteger as informações de seus clientes e usuários não só cumprem suas obrigações legais, mas também conquistam uma vantagem competitiva”, fortalecendo a confiança do público em seus serviços.

Entretanto, deve-se ressaltar que por já se encontrar na forma industrializada, a Inteligência Artificial, possui inúmeras variedades, tipos, versões e propósitos. Devido a este feito como produto, a fiscalização fica por vezes, marginalizada e excludente do processo de controle e supervisão. Posto isso, entende-se a necessidade de adaptação na regulamentação através de investimentos no âmbito promotor de segurança tecnológica.

A adesão a normas de proteção de dados, como LGPD no Brasil e o *General Data Protection Regulation* (GDPR) na União Europeia, é, atualmente, um elemento essencial nas estratégias de negócios e governança.

3.1.2. Propriedade Intelectual

A propriedade intelectual refere-se ao conjunto de direitos legais que protegem e preservam as criações da mente humana, como invenções, obras literárias, artísticas, *designs* ou qualquer outra criação abstrata humana seja artística ou comercial. Ela visa garantir que os criadores ou inventores possam ter o reconhecimento e a recompensa pelo uso de suas criações, proporcionando um incentivo para a inovação e o desenvolvimento, mas tem enfrentado desafios.

As leis de propriedade intelectual precisam ser constantemente atualizadas para refletir as mudanças tecnológicas e garantir que as criações não sejam utilizadas sem a devida autorização ou compensação ao criador.

A IA gera debates contudentes de onde parte a ideia de criação e a subjetividade que isso implica juntamente com a aceleração do processo que se torna cada vez mais superficial e menos propriamente humano. Sendo assim, a propriedade intelectual regida pelo Código Civil para reservar e restringir o privilégio de suas mentes pensantes contra plágios e fraudes fica vulnerável às intensas atividades inovadoras e incansáveis da IA.

É inegável entender o processo que a IA desempenha não somente no campo de execução das atividades, mas principalmente, na tendência em influenciar no campo criativo gerando assim uma homogeneização no espaço intelectual subtraindo para si qualquer demanda desde o processo inicial ao final de cada produção em que é inserida.

3.1.3. Proteção do Público Vulnerável

A proteção do público vulnerável em relação à IA é uma questão crucial, uma vez que essas tecnologias podem exacerbar desigualdades sociais e econômicas, especialmente quando não reguladas de forma adequada. Trata-se de crianças, idosos, pessoas com deficiência e populações de baixa renda que são frequentemente os mais afetados por decisões automatizadas que não levam em conta suas necessidades específicas.

Os algoritmos de IA, quando mal projetados ou não auditados, podem reforçar preconceitos e discriminação, resultando em exclusão ou marginalização desses grupos.

A falta de transparência no funcionamento de muitos sistemas e a dificuldade em compreender como as decisões são tomadas tornam esses indivíduos ainda mais suscetíveis a abusos e injustiças, tornando urgente a criação de políticas públicas que garantam uma proteção efetiva e inclusiva.

A falta de compreensão dos sistemas automatizados e a dificuldade em questionar decisões tomadas por algoritmos deixam essas populações à mercê de práticas injustas, discriminatórias e até perigosas. É essencial que haja uma regulação rigorosa, garantindo que a IA seja usada de maneira ética, transparente e que leve em consideração as necessidades específicas desses grupos. Somente com medidas eficazes de proteção será possível mitigar os danos e garantir um ambiente digital mais seguro para crianças, idosos e outros vulneráveis, respeitando seus direitos e dignidade.

3.2. CONTROLE E FISCALIZAÇÃO

O controle e a fiscalização da IA são essenciais para garantir que essas tecnologias sejam utilizadas de maneira ética, transparente e em conformidade com

as leis e direitos fundamentais. À medida que a IA se torna cada vez mais integrada em diversos setores, como saúde, finanças e segurança pública, surge a necessidade de mecanismos que monitorem e regulem sua aplicação.

A falta de fiscalização adequada pode levar ao uso indevido, como a discriminação algorítmica, a invasão de privacidade e a tomada de decisões automáticas sem responsabilidade clara. Nesse contexto, os governos e organismos internacionais devem desempenhar um papel ativo na criação e implementação de normas que assegurem a justiça e a transparência nos processos que envolvem IA.

A fiscalização deve envolver a participação ativa da sociedade civil, com a criação de canais de denúncia e mecanismos legais que permitam que abusos relacionados ao uso da IA sejam identificados e corrigidos.

Demais disso, a carência de fiscalização pode levar a uma sensação de impunidade entre as empresas que utilizam essas tecnologias, comprometendo a confiança do público.

Portanto, é irreparável que a fiscalização da seja realizada de forma colaborativa, envolvendo não apenas o setor público, mas também as organizações privadas, especialistas em ética digital e a sociedade em geral, com o objetivo de garantir que a evolução ocorra de maneira responsável, segura e alinhada aos direitos e interesses coletivos. Para Silva e Domingues (2024, p. 183):

A legislação criou a Autoridade Nacional de Proteção de Dados (ANPD), órgão responsável por fiscalizar o cumprimento da lei, aplicar sanções em caso de violações, e dirigir políticas públicas para a proteção de dados pessoais. A ANPD desempenha um papel crucial na interpretação da LGPD, orientando as organizações sobre como implementar as normas de forma eficaz.

Por sua vez, a Europa elevou a proteção dos dados pessoais à categoria de direito fundamental, tanto de forma individual quanto coletiva. Não é por acaso que a Europa e os Estados Unidos exercem uma considerável influência na formação das normas internacionais de proteção de dados, estabelecendo um marco regulatório que impacta globalmente. Para Brancher (2022):

O exemplo mais relevante de jurisdição que atualmente se baseia em uma abordagem setorial de regulação da proteção de dados pessoais é a dos Estados Unidos da América, país que, na esfera federal, não possui uma lei geral para Austrália e Canadá são outros exemplos de países que se guiam pela abordagem setorial. O segundo modelo propõe que um mesmo regime de proteção de dados se aplique a todos os tratamentos de dados pessoais

independentemente de elementos específicos. Desse modo, todas as entidades – públicas ou privadas – que tratem dados pessoais estarão, via de regra, sujeitas às mesmas obrigações, enquanto todo titular de dados terá acesso às mesmas garantias e direitos.

A grande vantagem dessa abordagem é que ela tende a atribuir maior segurança jurídica tanto às entidades que tratam dados pessoais – que passam a ter maior previsibilidade quanto às suas possibilidades e limites -, quanto aos titulares dos dados. Assim, embora regulações gerais requeiram um esforço generalizado de adequação, elas contribuem com um ambiente mais propício para o desenvolvimento econômico e tecnológico de sociedades e para a segurança de seus titulares.

Importante ressaltar que essa abordagem regulatória não impede que Estados baseados em leis gerais emanem também leis específicas que regulem o tratamento de dados pessoais de forma setorial. Na realidade, esse modelo híbrido é bastante recorrente, principalmente diante do fato de que muitos países já possuíam leis setoriais quando adotaram regulações gerais e, na maioria dos casos, não optaram pelo caminho da revogação das primeiras. Apenas como referência, na União Europeia, regula o tratamento de dados pessoais para fins de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais.

Em 2017, o Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC) iniciou o Plano Nacional de Internet das Coisas (IoT) que inclui a IA como uma das tecnologias-chave para o desenvolvimento de soluções inovadoras. A Estratégia Brasileira de Inteligência Artificial (EBIA) foi lançada em 2021 para impulsionar a pesquisa, o desenvolvimento e a aplicação da IA no País, com foco em áreas estratégicas como saúde, segurança, educação e agronegócio.

Tendo em vista a criação da setorização de proteção de dados, fica visível a necessidade de estender essa preocupação ao meio jurídico. Já existem ferramentas presentes nas litispendências, processos e recursos jurídicos. Tais movimentações judiciais devem obter para si sua parcela de programas detectadores de qualquer infração virtual ou pormenor que pode ocorrer virtualmente, razão pela qual alguns tribunais ainda não adotaram IA como ferramenta operacional.

O Brasil tem se preocupado também com as questões éticas relacionadas ao uso da IA e tem enfrentado desafios, como a falta de infraestrutura tecnológica em algumas regiões e a necessidade de investimentos em pesquisa e inovação. No entanto, o potencial de aplicação da IA no Brasil é vasto, especialmente nas áreas de agronegócio, saúde, educação e segurança pública.

Deve-se destacar a baixa oferta de profissionais qualificados para atuar no campo da IA.

No trabalho de pesquisa divulgado pelo CNJ (2023), 78 em 100 questionários relatam a falta de profissionais desta área. Como comprova o trecho de “Pesquisa de uso de inteligência artificial no Poder Judiciário” (CNJ, 2023, p. 40):

No entanto, os desafios não são triviais. A resistência interna e a necessidade de adaptação de processos estabelecidos são barreiras comuns, indicando que a mudança tecnológica requer também uma mudança cultural e organizacional. Além disso, a dificuldade em encontrar profissionais qualificados e as preocupações com a privacidade e segurança dos dados são desafios técnicos que precisam ser abordados para uma implementação bem-sucedida de IA.

Destaca-se que no Poder Judiciário, tribunais que lidam com refinação, volume e distribuição de processos, sendo eles mais litigiosos ou não, têm se mostrado mais abertos ao implemento da IA, principalmente a justiça Estadual, que detém o maior número de processos em trâmites de todas as categorias, dentre a Justiça Eleitoral, Justiça Federal, Justiça Superior e Justiça do Trabalho.

É indiscutível que houve um aumento na celeridade dos processos e uma degradação da lentidão em algumas áreas do Judiciário que tinha implementado a IA como suporte tecnológico no cotidiano jurídico. Veja o que publicou o CNJ (2023, p. 111):

Nota-se também um aumento na participação de equipes dedicadas em relação à pesquisa de 2022, provenientes dos próprios tribunais para o desenvolvimento desses projetos, indicando um crescente reconhecimento da importância das inovações tecnológicas na melhoria da eficiência e execução das atividades cotidianas do Judiciário. Também foi detectada uma maior quantidade de projetos finalizados e em andamento, com um decréscimo de projetos não iniciados em relação ao ano passado. Pesquisa de uso de Inteligência Artificial.

O CNJ tem implementado diversas iniciativas para regulamentar e monitorar o uso de IA visando garantir transparência, ética e eficiência. Seja projetos em cooperação com diversas universidades de renome no Brasil, o CNJ tem fomentado projetos novos de implementação e fiscalização da IA no Judiciário. Em fevereiro de 2025, o CNJ deliberou diversas regulamentações de seu uso no Poder Judiciário através de revisões e análises realizadas anteriormente, com o método de eficiência como promotor dessas deliberações. Essas ações refletem o compromisso do CNJ em promover o uso responsável e transparente da inteligência artificial no sistema judiciário, alinhando inovação tecnológica com os princípios fundamentais do direito.

CONCLUSÃO

A Inteligência Artificial (IA) apresenta desafios significativos para o Direito contemporâneo em termos de privacidade, proteção de dados e propriedade intelectual. Os grandes volumes de dados sensíveis processados por sistemas de IA, juntamente com o risco de ciberataques, tornam a segurança dos dados uma preocupação fundamental e pública.

A privacidade e a proteção de dados são direitos essenciais que devem ser preservados, especialmente considerando a digitalização crescente da sociedade.

Também não se sabe até onde a sociedade no estado atual terá controle sobre máquina que já possui capacidade para pensar e raciocinar de forma não somente a nível regular de um humano comum, mas capacitada para superar os limites que a mente humana possui. Essa apoteose tecnológica possui riscos, eventos e consequências éticas, sociais e intelectuais. O desafio se baseia no acompanhamento de diversos setores, principalmente o jurídico, postulando a exigência de transparência, liberalidade de fiscalização sobre todos os sistemas, variedade e ramificações da IA.

Para tal, a legislação precisa garantir que as empresas e desenvolvedores de IA implementem medidas de segurança robustas para evitar que suas tecnologias sejam empregadas de forma inadequada ou que fujam do controle.

No decorrer deste estudo verificou-se que a atuação da IA não necessita mais de debates de implementação, por mais que eles existam. O significado deste teste se deve ao enraizamento acelerado e velado dessa tecnologia que em menos de décadas encontra-se alastrada e com multidões dependentes de sua eficiência para suas ações comerciais, cotidianas, produtivas e até intelectuais. O debate de fato necessário, porém o uso de normas fiscalizadoras sobre a IA é imprescindível. Devido a autonomia soberba que atua, essa tecnologia precisa de supervisão, normas, e atos legislativos que andem paralelamente à sua autonomia. Supervisão, esta ou “autosupervisão”, como alguns cientistas já a definem como mente pensante autônoma e pasmem, independente.

As normas recentes refletem o crescente reconhecimento dos riscos representados pelos crimes digitais e a necessidade de punição e fiscalização. Sendo assim, tendo em vista os riscos apresentados, as opções viáveis de manutenção da

IA com a celeridade que a mesma proporciona às atividades humanas, é essencial que a fiscalização e controle cumpram um papel notável e explícito. Tendo em vista, essa necessidade, a criação de parâmetros éticos em todos os softwares de IA, assim como a classificação do nível de risco de cada sistema. Exigências como estas devem ser implementadas sob supervisão de órgãos e departamentos públicos ou privados responsáveis pela fiscalização de que os preceitos éticos, legais e normativos estão sendo respeitados e executados. Ademais, deve-se criar uma rede de transparência do uso de IA, de forma que o público tenha ciência da presença de Inteligência Artificial nas atividades e serviços que se dispõe a apresentar.

Portanto, a IA, por mais nova e arrebatadora precisa de delimitações no sentido que sua atuação não cause prejuízos, mas apenas benefícios. Apesar de ser extremamente útil e avançada, carece de base ética, social, normativa que assegurem suas atividades de forma que não promova retrocesso nas relações humanas. O desafio pode parecer meticuloso devido ao poder e autonomia que esta tecnologia já transporta e propaga globalmente. No entanto, a fiscalização não trata de refreios ou retrocesso, e sim a necessidade do paralelo tecnológico e ético que surte efeitos no âmbito jurídico, pois qualquer violação ou prejuízo a uma vida humana provoca o Direito e suas diretrizes. Com transparência, fiscalização e controle, a relação entre homem e máquina avança para que não seja uma distopia futura.

REFERÊNCIAS

- BRANCHER, Paulo Marcos Rodrigues. **Proteção internacional de dados pessoais**. Tomo Direito Internacional, Edição 1, Fevereiro de 2022. Disponível em: <https://enciclopediajuridica.pucsp.br/verbete/496/edicao-1/protecao-internacional-de-dados-pessoais>. Acesso em: 9 abr. 2025.
- BRANDÃO, Rodrigo. **Desenvolvimento da inteligência artificial no Brasil**. 2025. Disponível em: <https://cetic.br/media/docs/publicacoes/6/20240514085112/psi-ano-xvi-n-1-desenvolvimento-ia-brasil.pdf>. Acesso em: 9 abr. 2025.
- CARVALHO, Patrícia Heloisa de. **O “Marco Civil da Internet”: uma análise sobre a constitucionalidade do artigo 1**. 2017. Disponível em: <http://fdsm.edu.br/adm/artigos/6917c36392274c9b6393c7f7a7bddd1.pdf>. Acesso em: 9 abr. 2025.
- CONSELHO NACIONAL DE JUSTIÇA. **Pesquisa uso de inteligência artificial (IA) no Poder Judiciário: 2023**. Brasília: CNJ, 2024. 120 p. Disponível em: <https://bibliotecadigital.cnj.jus.br/jspui/handle/123456789/858>.
- DOMINGUES, Patricia Martinez; SILVA, Tainã Dias da; **Inteligência Artificial e Privacidade: Os desafios do Privacy by Design**. 2024. Artigo Universidade Federal de Minas Gerais, Belo Horizontw. 2024. Disponível em: <https://periodicos.ufmg.br/index.php/advances-kr/article/download/52813/44775/199635>. Acesso em 28, maio, 2025.
- FIGUEIREDO, Rudá. **CRIMES ELETRÔNICOS E LEI 14.155/2021**. 2021. Disponível em: https://www.mpba.mp.br/sites/default/files/biblioteca/criminal/artigos/codigo_penal_-_parte_especial/crimes_eletronicos_e_lei_14.155-2021.pdf. Acesso em 28, maio, 2025.
- GOMES, Dennis dos Santos. **Introdução à inteligência artificial**. 2010. Artigo Faculdades Associadas de Ariquemes- FAAr. Ariquemes, Rondônia. 2010. Disponível em: https://www.professores.uff.br/screspo/wp-content/uploads/sites/127/2017/09/ia_intro.pdf. Acesso em: 9 abr. 2025.
- HAUGELAND, John. **Artificial Intelligence: The Very Idea**. Massachusetts: The MITPress, 1985. Disponível: https://www.researchgate.net/publication/256121747_Artificial_intelligence_The_very_idea_J_Haugeland_MIT_Press_Cambridge_MA_1985_287_pp. Acesso em 28, maio, 2025.
- LIMA, Juliana Kelly Costa de; TROVÃO, Lidiana Costa de Sousa. **A Lei nº 12.737/2012 (Carolina Dieckmann) e seu impacto na sociedade para proteção de dados informáticos**. 2025. Disponível em: <https://revistaft.com.br/a-lei-n-12-737-2012-carolina-dieckmann-e-seu-impacto-na-sociedade-para-protecao-de-dados-informaticos/>. Acesso em: 9 abr. 2025.

MORAIS, Flávio Daniel Borges de; BRANCO, Valdec Romero Castelo. **A inteligência artificial: conceitos, aplicações e controvérsias**. 2023. Dissertação SIMPÓSIO INTERNACIONAL DE CIÊNCIAS INTEGRADAS DA UNAERP - CAMPUS GUARUJÁ, Ribeirão Preto, São Paulo. 2023. Disponível em: <https://www.unaerp.br/documentos/5528-a-inteligencia-artificial-conceitos-aplicacoes-e-controversias/file>. Acesso em: 9 abr. 2025.

Portal do Ministério Público da Bahia, **Crimes Eletrônicos e Lei 14.155/2021**, 2021. Ministério Público Da Bahia. Disponível em: https://www.mpba.mp.br/sites/default/files/biblioteca/criminal/artigos/codigo_penal_-_parte_especial/crimes_eletronicos_e_lei_14.155-2021.pdf. Acesso em: 9 abr. 2025.

RUSSEL, Stuart; NORVIG, Peter. Livro **Inteligência Artificial**. 2. Ed. Rio de Janeiro: Campos, 2004. Tradução da Terceira Edição. Disponível em: [https://www.kufunda.net/publicdocs/Intelig%C3%Aancia%20Artificial%20\(Peter%20Norvig,%20Stuart%20Russell\).pdf](https://www.kufunda.net/publicdocs/Intelig%C3%Aancia%20Artificial%20(Peter%20Norvig,%20Stuart%20Russell).pdf). Acesso em: 28, maio, 2025.

SAMPAIO, Rafael Cardoso; SABBATINI, Marcelo; LIMONGI, Ricardo; **Diretrizes para o uso ético e responsável da Inteligência Artificial Generativa**. 2024. Artigo, Universidade Estadual de Campinas, Campinas, São Paulo. 2024. <https://prpg.unicamp.br/wp-content/uploads/sites/10/2025/01/livro-diretrizes-ia-1.pdf>. Acesso em 19 maio 2025.

SANTOS, Marcelo Fonseca. **Inteligência artificial e o perfilamento de crianças e adolescentes: riscos e ações afirmativas para a proteção de dados**. 2025. Disponível em: https://magis.agej.com.br/inteligencia-artificial-e-o-perfilamento-de-criancas-e-adolescentes-riscos-e-acoes-afirmativas-para-a-protecao-de-dados/?utm_source=chatgpt.com. Acesso em: 9 abr. 2025.

SILVA, Gabriel Lange da; SOUZA, Luana Santos de; SOUZA, Ingrid Stéphanie Monteiro de. **Desafios e riscos de utilização inadequada da inteligência artificial como ferramenta de resolução de demandas no sistema judiciário**. 2025. Disponível em: <https://revistaft.com.br/desafios-e-riscos-de-utilizacao-inadequada-da-inteligencia-artificial-como-ferramenta-de-resolucao-de-demandas-no-sistema-judiciario/>. Acesso em: 9 abr. 2025.

Zendesk, **Qual é a origem da inteligência artificial? Onde tudo começou?** Portal Zendesk, Artigo. 2024 Disponível em: <https://www.zendesk.com.br/blog/qual-e-a-origem-da-inteligencia-artificial/>. Acesso em 28, maio, 2025.