INSTITUTO BRASILEIRO DE ENSINO, DESENVOLVIMENTO E PESQUISA
ESCOLA DE DIREITO E ADMINISTRAÇÃO
MESTRADO ACADÊMICO EM DIREITO

THAIS PARANHOS CAPISTRANO PEREIRA

EXPLORANDO OS LIMITES DA RESPONSABILIDADE CIVIL: O IMPACTO DO DESENVOLVIMENTO TECNOLÓGICO DOS PROCEDIMENTOS CIRÚRGICOS ROBÓTICOS

BRASÍLIA
2024

THAIS PARANHOS CAPISTRANO PEREIRA

EXPLORANDO OS LIMITES DA RESPONSABILIDADE CIVIL: O IMPACTO DO DESENVOLVIMENTO TECNOLÓGICO DOS PROCEDIMENTOS CIRÚRGICOS ROBÓTICOS

Dissertação apresentada como requisito parcial para obtenção do título de Mestra em Direito Constitucional, pelo Programa de Pós-Graduação em Direito do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa - IDP.

Orientador: Prof. Dr. Nelson Rosenvald.

BRASÍLIA

2024

Cutter Pereira, Thais Paranhos Capistrano
Título: Explorando os limites da responsabilidade civil: o impacto do desenvolvimento tecnológico dos procedimentos cirúrgicos robóticos/ Thais Paranhos Capistrano Pereira. – Brasília: IDP, 2024.

127 p.
Inclui bibliografia.

Dissertação de Mestrado – Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa – IDP, Curso de Mestrado em Direito Constitucional, Brasília, 2024.
Orientador: Prof. Dr. Nelson Rosenvald.
1. Responsabilidade Civil; 2. Inteligência Artificial; 3. Cirurgia Robótica; 4. *Accountability*. I Explorando os limites da responsabilidade civil: o impacto do desenvolvimento tecnológico dos procedimentos cirúrgicos robóticos.

CDD: XXX

Ficha catalográfica elaborada pela Biblioteca Ministro Moreira Alves
Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa

THAIS PARANHOS CAPISTRANO PEREIRA

EXPLORANDO OS LIMITES DA RESPONSABILIDADE CIVIL: O IMPACTO DO DESENVOLVIMENTO TECNOLÓGICO DOS PROCEDIMENTOS CIRÚRGICOS ROBÓTICOS

Dissertação de Mestrado apresentada como requisito parcial para obtenção do título de Mestre em Direito Constitucional pelo Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP).

Orientador: Prof. Dr. Nelson Rosenvald.

Brasília, 02 de julho de 2024

BANCA EXAMINADORA

Prof. Dr. Nelson Rosenvald
Orientador
Pós-Doutorado em Direito Civil na Universidade Roma Tre/ Italia (2011) e Pós Doutorado em Direito Societário pela Universidade de Coimbra (2015).
Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa - IDP

Prof. Dr. Bruno Torquato Zampier Lacerda
Doutor Direito Privado - PUC Minas
Faculdade Supremo IDDE – Belo Horizonte

Prof. Dr. José Luiz de Moura Faleiros Júnior
Doutor Direito Privado - Universidade de São Paulo (USP)
Faculdade Milton Campos (IES) – Belo Horizonte

Prof. Dr. Ilton Norberto Robl Filho
Pós-Doutorado (2015) em Direito Constitucional pela Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS)
Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa - IDP

Ao meu eterno incentivador, Dr. Roland Montenegro Costa (*in memorian*).

AGRADECIMENTOS

Gostaria de expressar minha profunda gratidão ao Dr. Roland Montenegro Costa, cuja inspiração e motivação foram fundamentais para despertar meu interesse no fascinante campo das cirurgias robóticas.

Agradeço também à professora Drª Cristiane Maria Tonetto Godoy, cujas contribuições valiosas enriqueceram significativamente minha pesquisa e trouxeram novas perspectivas ao meu estudo.

Ao professor Dr. Felipe Braga Netto, agradeço por todas as valiosas discussões, conselhos e sugestões que enriqueceram significativamente este estudo. Foi um privilégio ter tido a oportunidade de aprender e crescer com suas contribuições.

Meu reconhecimento sincero ao meu orientador Dr. Nelson Rosenvald, e aos Professores Doutores, Bruno Zampier, Ilton Robl Filho, José Luiz Faleiros Júnior e Filipe Medon, cujos conhecimentos enriqueceram significativamente o conteúdo e a qualidade minha pesquisa.

Aos meus colegas de turma, em especial às minhas colegas Lúcia Teixeira Ferreira e Luana Esteche que estiveram comigo como pesquisadoras na Universidade de Granada, sou grata pela troca de ideias e apoio mútuo ao longo desta jornada.

Finalmente, minha gratidão eterna aos meus pais José e Avani e à minha filha Ana Laura, cujo amor incondicional e suporte constante foram a base que sustentou meus esforços e conquistas.

O gênero humano está perdendo a fé na narrativa liberal que dominou a política global em décadas recentes, justamente quando a fusão da biotecnologia com a tecnologia da informação nos coloca diante das maiores mudanças com que o gênero humano já se deparou.

(HARARI, 2018, p. 19)

RESUMO

A presente dissertação aborda a responsabilidade civil no contexto da crescente autonomia das inteligências artificiais (IA), com foco específico nas cirurgias robóticas. Atualmente a implementação de robôs cirurgiões, apesar da eficiência e precisão nos procedimentos cirúrgicos, também levanta questões éticas e legais significativas. A necessidade de alinhar a programação dos robôs com os valores humanos é fundamental para garantir que tais sistemas operem para o benefício da sociedade, minimizando, assim, os riscos e consequências indesejadas. Nesse contexto, objetivo central dessa pesquisa foi compreender os desafios éticos e jurídicos relacionados ao Código Civil (CC) e ao Código de Defesa do Consumidor (CDC) no contexto da inteligência artificial autônoma, em especial, dos cirurgiões robóticos. A metodologia utilizada foi qualitativa e exploratória, envolvendo análise comparativa de normativas dos Estados Unidos da América (EUA) e da União Europeia (UE), além da análise da legislação brasileira sob a ótica dos riscos da IA. Como resultado, foi possível perceber as diferenças nos marcos regulatórios entre EUA e UE, que refletem as diversas abordagens políticas e éticas, exigindo um diálogo contínuo entre desenvolvedores de tecnologia, legisladores e o público para a formação de um consenso global. O que pode ser observado é que a União Europeia tem sido mais proativa e firme em suas recomendações e regulamentações sobre a IA, embora muitas dessas normas sejam consideradas *soft laws.* A UE foca mais em regulamentações específicas para IA de alto risco, enquanto os EUA favorecem uma governança mais abrangente que exige ações específicas das empresas de tecnologia. No que tange a legislação brasileira, a LGPD adiciona uma camada de complexidade ao garantir a proteção de dados pessoais dos pacientes, enfatizando a necessidade de transparência e *accountability* por parte dos operadores desses sistemas. Na mesma linha, a Resolução n.º 2.311/2022 do Conselho Federal de Medicina (CFM) aponta que é fundamental os pacientes receberem todas as informações necessárias sobre os riscos, benefícios e alternativas às cirurgias robóticas. Assim, a responsabilidade civil pode ser envolvida se o consentimento informado não for adequadamente obtido. Ademais, esse estudo destacou que os fabricantes e desenvolvedores de sistemas inteligentes podem ser responsabilizados, mesmo se eles empregarem a tecnologia mais avançada disponível a época, e que, inicialmente, não apresentava defeitos evidentes, isso ao lançar o produto no mercado. Ressalta-se a importância da explicabilidade e da *accountability* em sistemas de IA, com um olhar detalhado sobre a cirurgia robótica. Como considerações finais, essa pesquisa aponta que, embora as legislações brasileiras atuais ofereçam alguma proteção, existe necessidade de ajustes e maior clareza nas responsabilidades por meio da *accountability* e explicabilidade para garantir a segurança no uso de IA autônoma na medicina, bem como a redução do *quantum* indenizatório na medida em que o agente tenha investido em *compliance* para evitar as consequências indesejadas e prestado a devida *accountability*.

Palavras-chave: Responsabilidade Civil; Inteligência Artificial; Cirurgia Robótica; *Accountability*.

ABSTRACT

The present dissertation addresses civil liability in the context of the increasing autonomy of artificial intelligence (AI), with a specific focus on robotic surgeries. Currently, the implementation of surgical robots, despite their efficiency and precision in surgical procedures, also raises significant ethical and legal issues. The need to align the programming of robots with human values is fundamental to ensure that such systems operate for the benefit of society, thereby minimizing risks and undesirable consequences. In this context, the central objective of this research was to understand the ethical and legal challenges related to the Civil Code (CC) and the Consumer Protection Code (CDC) in the context of autonomous artificial intelligence, particularly robotic surgeons. The methodology used was qualitative and exploratory, involving a comparative analysis of regulations from the United States of America (USA) and the European Union (EU), in addition to analyzing Brazilian legislation from the perspective of AI risks. As a result, it was possible to perceive the differences in regulatory frameworks between the USA and the EU, which reflect diverse political and ethical approaches, requiring ongoing dialogue between technology developers, legislators, and the public to form a global consensus. It was observed that the European Union has been more proactive and firm in its recommendations and regulations regarding AI, although many of these norms are considered soft laws. The EU focuses more on specific regulations for high-risk AI, while the USA favors broader governance that requires specific actions from technology companies. Regarding Brazilian legislation, the General Data Protection Law (LGPD) adds a layer of complexity by ensuring the protection of patients' personal data, emphasizing the need for transparency and accountability by operators of these systems. Similarly, Resolution No. 2.311/2022 of the Federal Council of Medicine (CFM) states that it is essential for patients to receive all necessary information about the risks, benefits, and alternatives to robotic surgeries. Thus, civil liability may be involved if informed consent is not adequately obtained. Furthermore, this study highlighted that manufacturers and developers of intelligent systems can be held liable, even if they employ the most advanced technology available at the time, which initially showed no evident defects upon market launch. The importance of explainability and accountability in AI systems, with a detailed look at robotic surgery, is emphasized. As final considerations, this research indicates that, although current Brazilian legislation offers some protection, there is a need for adjustments and greater clarity in responsibilities through accountability and explainability to ensure the safe use of autonomous AI in medicine. Additionally, it points to the reduction of compensation amounts to the extent that the agent has invested in compliance to avoid undesirable consequences and provided due accountability.

Keywords: Civil liability; Artificial Intelligence; Robotic Surgery; Accountability.

LISTA DE ABREVIATURAS E SIGLAS

AAA	*Algorithmic Accountability Act*
ADI	Ação Direta de Inconstitucionalidade
ADS	*Automated Decision Systems*
AGI	*Artificial General Intelligence*
ANI	*Artificial Narrow Intelligence*
ASI	*Artificial Super Intelligence*
CC	Código Civil
CDC	Código de Defesa do Consumidor
CNMP	Conselho Nacional do Ministério Público
CF	Constituição Federal
COMEST	Comissão Mundial para Ética do Conhecimento Científico e Tecnológico da UNESCO
DARPA	*Defense Advanced Research Projects Agency*
DMA	*Digital Market Act*
DSA	*Digital Service Act*
FTC	*Federal Trade Commission*
FDA	*Food and Drug Administration*
FRIA	*Fundamental Rights Impact Assessment*
GDPR	*General Data Protection Regulation of the European Parliament*
IA	Inteligência Artificial
LGPD	Lei Geral de Proteção de Dados
ML	*Machine learning*
OCDE	Organização para a Cooperação e Desenvolvimento Econômico
OECD	*Organisation for Economic Cooperation and Development*
PUMA	*Programmable Universal Machine for Assembly*
RASDS	*Reference Architecture for Space Data Systems*
RGPD	Regulamento Geral de Proteção de Dados
SIA	Sistema Nacional de Regulação e Governança de Inteligência Artificial
SUS	Sistema Único de Saúde
STJ	Superior Tribunal de Justiça
TICs	Tecnologias da Informação e Comunicação
XAI	*Explainable Artificial Intelligence*

SUMÁRIO

INTRODUÇÃO.....1

1 DA INTELIGÊNCIA ARTIFICIAL À ROBÓTICA NA MEDICINA.....5

1.1 FUNDAMENTOS CONCEITUAIS PARA ENTENDER A INTELIGÊNCIA ARTIFICIAL E ALGORITMOS.....6

1.2 TIPOS DE INTELIGÊNCIA ARTIFICIAL, APRENDIZADO DAS MÁQUINAS E ROBÔS.....11

1.3 AVANÇOS DA INTELIGÊNCIA ARTIFICIAL NA MEDICINA: O IMPACTO TRANSFORMADOR DOS ROBÔS CIRÚRGICOS.....14

1.3.1 Robôs Cirúrgicos: Até Da Vinci evolução dos robôs cirúrgicos.....16

2 IMPLICAÇÕES JURÍDICAS DO EMPREGO DE INTELIGÊNCIA ARTIFICIAL E A RESPONSABILIDADE CIVIL.....20

2.1.....EXPLORANDO OS CONCEITOS DA RESPONSABILIDADE CIVIL NA ERA DAS NOVAS TECNOLOGIAS.....20

2.1.1 *Liability*.....26

2.1.2 *Responsibility*.....28

2.1.3 *Accountability*.....30

2.1.4 *Answerability* - Explicabilidade.....33

3 NEXO CAUSAL NA ERA DA INOVAÇÃO: ANÁLISE JURÍDICA DA CIRURGIA ROBÓTICA E A TEORIA DO RISCO DO DESENVOLVIMENTO.....37

3.1 CONSIDERAÇÕES INICIAIS SOBRE O NEXO CAUSAL.....38

3.2 NEXO CAUSAL E IA AUTÔNOMA.....42

3.3 DO NEXO CAUSAL NA ÁREA DA SAÚDE.....45

3.3.1 Do dever de informação.....48

3.4 TEORIA DO RISCO DO DESENVOLVIMENTO.....51

4 PREVENÇÃO E GESTÃO DOS RISCOS NO DESENVOLVIMENTO DA INTELIGÊNCIA ARTIFICIAL.....58

4.1..... GERENCIAMENTO DE RISCOS DA IA PELAS NORMATIVAS DOS ESTADOS UNIDOS.....61

4.2 GERENCIAMENTO DE RISCOS DA IA PELAS NORMATIVAS DA UNIÃO EUROPEIA.....66
4.3 ...ESTUDO COMPARADO ENTRE O GERENCIAMENTO DE RISCOS DA IA ENTRE AS NORMATIVAS DOS EUA E DO PARLAMENTO EUROPEU.....71

5 OS PARÂMETROS ATUAIS DA RESPONSABILIDADE CIVIL NA UTILIZAÇÃO DA IA NO CONTEXTO BRASILEIRO.....76
5.1 LEGISLAÇÃO BRASILEIRA SOB O OLHAR DOS RISCOS DA INTELIGÊNCIA ARTIFICIAL.....76
5.2 RESPONSABILIDADE CIVIL E IA CORRENTES DOUTRINÁRIAS.....82
5.3 O DEVER DE INDENIZAR O DANO DECORRENTE DE UMA CIRURGIA ROBÓTICA, A EXPLICABILIDADE, A *ACCOUNTABILITY* E *COMPLIANCE*.....91
5.4 ALGUNS DIRECIONAMENTOS DE COMO INDENIZAR.....95

6 CONSIDERAÇÕES FINAIS….....98

REFERÊNCIAS.....104

INTRODUÇÃO

Como pesquisadora e profissional da área jurídica, minha trajetória acadêmica e profissional tem sido permeada pelo interesse na interface entre o Direito Civil, especialmente a responsabilidade civil, e os avanços tecnológicos. Graduada em Direito com habilitação na área civil e com uma monografia de conclusão de curso voltada para o Direito do Consumidor, minha jornada acadêmica reflete um profundo interesse na proteção dos direitos individuais. Além disso, minha experiência profissional, na área cível do Ministério Público Federal, proporcionou-me uma compreensão aprofundada das complexidades jurídicas enfrentadas na prática. A combinação dessas experiências acadêmicas e profissionais culminou em um forte interesse em cursar o Programa de Pós-Graduação Stricto Sensu em Direito Constitucional - Mestrado Acadêmico em Direito Constitucional do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP - Brasília), onde pude aprofundar meus conhecimentos na área cível.

Destarte, foi a partir de um encontro fortuito com o cirurgião Roland Montenegro Costa e de nossa conversa sobre a responsabilidade legal diante dos riscos inerentes ao desenvolvimento tecnológico, no contexto das inteligências artificiais autônomas utilizadas em cirurgias robóticas, que aconteceu a inspiração para uma temática a ser estudada. A partir dessa conversa, surgiu o interesse de compreender quais os riscos poderiam ser considerados uma excludente da reparação de danos ou consequências indesejadas advindas da Inteligência Artificial (IA), culminando no problema de pesquisa dessa Dissertação.

Algoritmos, inteligência artificial e redes sociais, expressões estas que antes eram desconhecidas da população, hoje fazem parte do nosso cotidiano e são fruto do grande impacto dos avanços tecnológicos, principalmente, no campo da comunicação. Um sistema de IA é uma entidade baseada em computador que, para fins claramente definidos ou não, processa dados recebidos para gerar *outputs* como previsões, conteúdos, recomendações ou decisões. Esses resultados têm o potencial de impactar ambientes tanto físicos quanto digitais. Os sistemas de IA diferem em seus graus de autonomia e capacidade de adaptação após serem implementados. Esta definição foi debatida em meados de outubro de 2023 durante as reuniões do Comitê de Política da Economia Digital e do Grupo de Trabalho sobre Governança da Inteligência Artificial da OCDE. Os *insights* dessas discussões estão programados para orientar a futura Lei de IA da União Europeia.

Essa nova realidade tem provocado diversas transformações, tanto nas relações sociais, na estrutura econômica mundial, campo político e também na área da saúde. Logo, a

utilização de robôs em cirurgias tem se tornado uma prática cada vez mais comum em hospitais ao redor do mundo, oferecendo procedimentos mais precisos e menos invasivos. No entanto, recentes incidentes, envolvendo erros cometidos por esses sistemas automatizados, têm levantado preocupações sobre a segurança e eficácia desses procedimentos.

Exemplificando, em Boca Raton, na Flórida, um robô cirúrgico causou a morte de uma paciente ao queimar seu intestino delgado durante um procedimento para tratar câncer de cólon. O esposo da vítima entrou com um processo judicial, alegando que a fabricante do robô Da Vinci, a Intuitive Surgical Inc., não alertou sobre os riscos associados às falhas no equipamento, o que resultou em danos irreparáveis (Ferreira, 2024). Paralelamente, no Freeman Hospital, em Newcastle, Inglaterra, um incidente semelhante ocorreu durante uma cirurgia cardíaca em 2015. Stephen Pettitt, de 69 anos, faleceu devido a um erro cometido pelo robô durante a substituição da válvula mitral. O septo interatrial foi perfurado acidentalmente, causando uma hemorragia fatal. A equipe médica admitiu que mais testes deveriam ter sido realizados com o robô antes de sua utilização em cirurgias tão delicadas (Moreira; Fernando, 2018).

Outra notícia envolvendo dano causado por cirurgião robô, aconteceu em março de 2009, em Tacoma, Washington. Erin Izumi, uma mulher de 30 anos, passou por uma cirurgia assistida por robótica para tratar endometriose. Após a operação, descobriu-se que seu cólon e reto haviam sido perfurados, levando-a a ser hospitalizada por cinco semanas e passar por diversos procedimentos para reparar o dano. (Makary; Daniel M.,2016).

Conforme revelado por um estudo publicado no "Journal for Quality Healthcare", foram identificadas 174 lesões graves e 71 mortes relacionadas à cirurgia com o sistema Da Vinci. A utilização de cirurgia robótica tem crescido significativamente, com um aumento de mais de 400% nos EUA entre 2007 e 2011, e cerca de 1.400 sistemas Da Vinci adquiridos pelos hospitais. Um estudo de 2010 revelou que mais da metade dos cirurgiões entrevistados anonimamente relataram situações de falhas operacionais irreversíveis durante o uso do robô Da Vinci. Além disso, constatou-se que as mulheres têm uma probabilidade maior de serem prejudicadas durante os procedimentos robóticos (Makary; Daniel M.,2016).

Esses casos destacam a importância de uma avaliação rigorosa e contínua dos sistemas robotizados antes de sua aplicação em procedimentos cirúrgicos, especialmente aqueles de alto risco. Apesar das promessas de precisão e segurança, os erros cometidos pelos robôs podem ter consequências indesejáveis e devastadoras para os pacientes e suas famílias.

Outrossim, a crescente utilização dos meios digitais por toda sociedade e dos mecanismos inteligentes autônomos demandam a necessidade de melhor informação,

transparência e segurança. Dessa feita, à medida que esses recursos tecnológicos se proliferam, surgem questões éticas e legais complexas, isso quando se trata da responsabilidade por danos causados por inteligência artificial em cirurgias robóticas.

A responsabilidade civil, tradicionalmente baseada na ação humana, enfrenta novos desafios diante da crescente autonomia das inteligências artificiais. Desse modo, é primordial reavaliar os conceitos tradicionais de responsabilidade civil, sobretudo, no contexto das cirurgias robóticas, já que os sistemas inteligentes assumem um papel mais ativo na tomada de decisões médicas e podem estar sujeitos a falhas ou comportamentos inesperados.

Nessa perspectiva, ao extrapolarmos para a diversidade de tipos de IA reflete-se a necessidade de uma abordagem ética e jurídica cuidadosa. Os desenvolvedores e os responsáveis pela implementação de sistemas de IA têm a responsabilidade ética de comunicar claramente os possíveis perigos associados ao uso dessas tecnologias. Igualmente, os usuários também têm o direito de serem informados sobre como as decisões são tomadas por sistemas de IA.

A transparência sobre as capacidades e limitações das máquinas inteligentes é essencial para evitar danos e expectativas irreais. O entendimento claro dos impactos e responsabilidades associados a cada tipo de IA torna-se necessário para moldar um futuro onde a inteligência artificial não apenas aprimora, mas também preserva os valores fundamentais da sociedade.

Nesse contexto, uma questão central que surge é compreender os desafios éticos e jurídicos relacionados à responsabilidade civil no contexto da inteligência artificial autônoma, em especial, nesse trabalho, dos cirurgiões robóticos. Assim, o presente estudo tem como problema de pesquisa a seguinte indagação: O Código Civil e o Código de Defesa do Consumidor são capazes de garantir a proteção dos direitos e interesses das partes envolvidas, a fim de promover um ambiente seguro e responsável para o desenvolvimento e implementação da inteligência artificial, em especial, dos cirurgiões robóticos?

Assim, a presente pesquisa tem como **objetivo geral** compreender os desafios éticos e jurídicos relacionados ao Código Civil e ao Código de Defesa do Consumidor no contexto da inteligência artificial autônoma, em especial, dos cirurgiões robóticos. E atende os **objetivos específicos:** i. Realizar um estudo comparado entre o gerenciamento de riscos da IA entre as normativas dos EUA e do Parlamento Europeu; ii. Analisar a legislação brasileira sob o olhar dos riscos da inteligência artificial em cirurgias robóticas, bem como o diálogo existente sobre as novas premissas da responsabilidade civil, em particular, sobre a *accountability*; e iii Explorar possíveis alternativas à luz do Código Civil e do Código de Defesa do Consumidor

para promover um ambiente seguro e responsável para o desenvolvimento e implementação da inteligência artificial em cirurgias robóticas.

Como aporte metodológico se fez uso de uma abordagem qualitativa, de cunho exploratório. Essa abordagem será realizada em função da interdisciplinariedade da temática, considerando as áreas de Direito Constitucional, Civil, Consumidor e as Ciências da Computação. Desse modo, foram utilizadas fontes bibliográficas competentes, legislações internacionais e nacionais, jurisprudências e compêndios conceituais acerca da temática pesquisada, buscando o arcabouço conceitual necessário para a discussão.

Ademais, foi empregado o método comparativo para examinar os documentos legislativos da Europa e dos Estados Unidos, relevantes para a temática abordada quanto ao gerenciamento dos riscos envolvendo às IA. Cabe destacar, que sobre as definições de inteligência artificial e responsabilidade civil, utilizar-se-á como marco teórico a doutrina de Nelson Rosenvald e Felipe Braga Netto (2024), auxiliando assim, na compreensão dos fenômenos relacionados ao objeto de pesquisa.

A dissertação encontra-se dividida em cinco capítulos, além da Introdução e Considerações Finais. O Capítulo 1 intitulado “Da integração da inteligência artificial e a robótica na medicina” analisa os fundamentos conceituais para entender a inteligência artificial e algoritmos, bem como o impacto transformador dos robôs cirúrgicos.

Em seguida, o Capítulo 2 intitulado “Implicações jurídicas do emprego da inteligência artificial e responsabilidade civil” tem como objetivo abordar as novas premissas da responsabilidade civil na era das novas tecnologias. No Capítulo 3 nominado “Nexo causal na era da inovação: análise jurídica da cirurgia robótica e a teoria do risco do desenvolvimento” se faz uma análise sobre o nexo causal na área da saúde, ressaltando o dever de informação, bem como fará uma abordagem sobre a teoria do risco do desenvolvimento.

Posteriormente, o quarto capítulo denominado “Prevenção e gestão dos riscos no desenvolvimento da inteligência artificial” descreve o gerenciamento de riscos da IA pelas normativas dos EUA e do Parlamento Europeu, finalizando com um estudo comparado entre as normativas. Por fim, o Capítulo 5 chamado “Os parâmetros atuais da responsabilidade civil na utilização da IA no contexto brasileiro” analisa a legislação brasileira sob o olhar dos riscos da inteligência artificial em cirurgias robóticas. Nas considerações finais, retomarei os principais achados nesta pesquisa e ponderações sobre IA, robôs cirúrgicos e responsabilidade civil no Brasil.

1 DA INTELIGÊNCIA ARTIFICIAL À ROBÓTICA NA MEDICINA

Na esfera jurídica, a inteligência artificial (IA) é comumente concebida como uma ferramenta (*AI as tool*), uma criação humana sujeita ao controle humano. No entanto, seu impacto transcende os limites legais, adentrando as complexas interações do comportamento humano na era digital. Algoritmos, impulsionados por tecnologias como aprendizado de máquina e aprendizado profundo, têm a capacidade singular de identificar padrões de comportamento online, possibilitando a compreensão de desejos, necessidades e comportamentos. Isso facilita a personalização de produtos, serviços e experiências humanas (Chaves, 2017).

O crescente uso da inteligência artificial abrange uma ampla gama de aplicações, desde assistentes virtuais em dispositivos móveis até sistemas robóticos cirúrgicos e veículos autônomos. Ao explorarmos a natureza da IA e suas implicações éticas para compreender seu impacto nos direitos fundamentais, é essencial considerar o desenvolvimento desses sistemas de maneira alinhada aos valores humanos, garantindo confiança (Dignum, 2019).

A IA possui um potencial significativo para proporcionar precisão, eficiência, economia de custos e ideias inovadoras em uma variedade de atividades humanas. Os sistemas inteligentes conseguem armazenar e processar grandes volumes de dados de maneira eficiente, proporcionando *insights* valiosos e acelerando a tomada de decisões, uma vez que, dependendo do tipo de inteligência artificial e do algoritmo envolvidos, há capacidades decisórias humanas que foram passadas aos computadores.

Além disso, a autonomia dos sistemas inteligentes suscita preocupações sobre segurança e responsabilidade. Aliás, como pondera Dignum (2019), o impacto da IA não se restringe apenas às direções de pesquisa e desenvolvimento, mas também a sua introdução na sociedade, influenciando o trabalho, bem-estar, interações sociais, saúde e distribuição de renda. Lidar com essas questões requer considerar implicações éticas, legais, sociais e econômicas.

Contudo, como toda ferramenta poderosa, a inteligência artificial também apresenta desafios e riscos que merecem atenção. Entre as inquietações geradas pelo desenvolvimento tecnológico as principais que objetivam este estudo são a IA como robô, ferramenta (*Robot as tool*). Para isso, necessário se faz abordar as bases conceituais a fim de melhor compreender proativamente os desafios associados ao uso dessas tecnologias que será realizado nos próximos itens.

1.1 FUNDAMENTOS CONCEITUAIS PARA ENTENDER A INTELIGÊNCIA ARTIFICIAL E ALGORITMOS

Falar em inteligência artificial e não mencionar Issac Asimov, é não conhecer o assunto. Conhecido escritor russo, naturalizado norte-americano, Asimov escreveu algumas importantes histórias sobre robôs, descrevendo a interação dos humanos com os robôs. Como em “Robbie”, onde uma criança ama sua babá robô. Também podem ser lembrados os contos “Razão” em que um robô se transforma em um religioso, e, ainda, “Mentiroso”, história de Asimov sobre um robô que consegue ler a mente humana (Asimov, 2014).

A partir de seus contos literários, o autor, supracitado, escreve as famosas e tão citadas Três Leis da Robótica no seu livro “Eu, robô”, em seu quarto conto chamado “Andando em círculos”. Apesar de não terem natureza normativa, as Três Leis da Robótica são tidas como princípios éticos basilares para o desenvolvimento responsável da tecnologia. Asimov assim as descreve:

> A) um robô não pode ferir um ser humano ou, por omissão, permitir que um ser humano sofra algum mal;
> B) um robô deve obedecer às ordens que lhe sejam dadas por seres humanos, exceto nos casos em que tais ordens contrariem a Primeira Lei;
> C) um robô deve proteger sua própria existência, desde que tal proteção não entre em conflito com a Primeira e a Segunda Leis (Asimov, 2014, p. 2).

Um tempo depois, o autor definiu a Quarta Lei, conhecida como “Lei Zero”, em razão de seu caráter anterior as demais leis. Segundo esta lei, “um robô não pode fazer mal à humanidade e, nem por omissão, permitir que ela sofra algum mal” (Asimov, 2002, p.181).

Por outro lado, para os autores Shabbir e Anwer (2015) a IA foi originada na Segunda Guerra Mundial com os estudos de Alan Turing para a decodificação de mensagens nazistas. Turing (1950) cunhou o termo inteligência artificial em sua obra Computacional Machinery and Intelligence em 1950. O pesquisador, matemático, lógico e criptoanalista britânico, é uma figura seminal na história da inteligência artificial. Embora Turing não tenha desenvolvido explicitamente a IA, suas ideias e contribuições tiveram um impacto significativo no campo acadêmico.

Vale lembrar também que as contribuições de Turing foram importantes para os estudos acerca da possibilidade de uma máquina processar informações e gerar respostas tais como um ser humano. Aliás, o pesquisador é mais conhecido por conceber a "Máquina de Turing", um dispositivo teórico que modela o funcionamento de um computador. Esse conceito é fundamental para a teoria da computação e é frequentemente utilizado para entender os limites e a capacidade de algoritmos e computadores (Cozman, 2021).

Em 1950, Turing propôs o "Teste de Turing" (*Entscheidungsproblem*) em seu artigo "Computing Machinery and Intelligence". Esse teste propôs uma maneira de avaliar a inteligência de uma máquina, se uma máquina pudesse realizar uma conversa de forma indistinguível de um humano, essa poderia ser considerada inteligente (Turing, 1950). Embora, o termo "Inteligência Artificial" tenha sido cunhado após a morte de Turing, suas ideias influenciaram diretamente o desenvolvimento da IA. O Teste de Turing, em particular, estimulou muitos pesquisadores a buscar métodos para criar máquinas que pudessem imitar o pensamento humano (Doneda, *et al*, 2018).

Durante a Segunda Guerra Mundial, foi desenvolvido um papel importante por Turing no esforço de guerra britânico, pois liderava a equipe que quebrava o código da máquina de criptografia alemã Enigma. A sua experiência em criptoanálise contribuiu indiretamente para o desenvolvimento de técnicas que mais tarde seriam fundamentais para a IA. Assim, embora ele não tenha desenvolvido diretamente a IA, as suas contribuições para a teoria da computação e suas ideias sobre máquinas inteligentes moldaram o pensamento e influenciaram o campo da inteligência artificial de maneiras profundas (Turing, 1950).

John McCarthy (2007) é conhecido como pai da IA devido à sua contribuição significativa para o desenvolvimento e promoção da IA como uma disciplina acadêmica e científica. O autor, define como a disciplina que se dedica à ciência e à engenharia de criar máquinas inteligentes, incluindo programas de computador inteligentes. Embora esteja conectada à tarefa de usar computadores para compreender a inteligência humana, a IA não está restrita aos métodos que podem ser observados na biologia (McCarthy, 2007).

McCarthy cunhou o termo "Inteligência Artificial" em uma conferência de 1956 na Universidade de Dartmouth, onde reuniu alguns dos pioneiros no campo da IA, embora o primeiro trabalho reconhecido como IA tenha sido desenvolvido por Warren McCulloch e Walter Pitts em 1943. Aquele evento em Dartmouth é amplamente considerado como um marco importante no início da pesquisa formal em IA (Cozman, 2021).

McCarthy também é conhecido por desenvolver a linguagem de programação LISP (List Processing), que desempenhou um papel fundamental no desenvolvimento de sistemas de IA. O LISP é uma das linguagens mais antigas ainda em uso hoje, e sua flexibilidade o tornou adequado para a implementação de algoritmos de IA. Além disso, McCarthy fez várias contribuições teóricas para o campo da IA incluindo o desenvolvimento do cálculo de predicados de primeira ordem, que é fundamental para a representação de conhecimento em sistemas de IA (Cozman, 2021).

Em uma definição mais contemporânea, a inteligência artificial é entendida como a

capacidade de um ser não natural fazer escolhas por meio de um processo de avaliação (Turner, 2019). Existem certas características que distinguem o sistema de inteligência artificial como tal, conforme Norvig e Russell (1995, p. 16) em seu livro "Inteligência Artificial: uma abordagem moderna", identificam as quatro principais categorias nas quais a inteligência artificial é geralmente conceituada: "sistemas que pensam como humanos", "sistemas que agem como humanos", "sistemas que pensam de maneira racional" e "sistemas que agem de maneira racional". Em relação aos aspectos que a singularizam e conferem-lhe uma racionalidade análoga aos seres humanos.

Por sua vez, Winston (1993) argumenta que há diversas maneiras de definir inteligência artificial, descrevendo-a como o estudo da computação que capacita os sistemas a perceber, raciocinar e agir. É importante notar que muitas máquinas são controladas por interfaces de comando, o que vincula suas ações à vontade do emissor ou proprietário. Por outro lado, algumas máquinas demonstram um nível mais baixo de interatividade, exibindo maior autonomia em relação ao ser humano. Assim, a maneira como as máquinas conduzem suas atividades varia entre sistemas com alta interatividade com o operador-usuário, geralmente obedecendo às suas instruções, e sistemas com baixa interatividade com o operador-usuário, frequentemente demonstrando capacidade autônoma na execução das tarefas.

No âmbito legal, a IA é comumente encarada como uma ferramenta, um artefato criado e controlado por seres humanos. Contudo, sua influência transcende as barreiras jurídicas, penetrando nas intricadas teias do comportamento humano na era digital.

A personalização, oriunda da análise algorítmica, culmina em interações mais relevantes e satisfatórias. Recomendações personalizadas, assistentes virtuais, e chatbots, como exemplificado pelo ChatGPT e Dall-E, que criam imagens realísticas, são testemunhos tangíveis do potencial transformador da IA no cotidiano digital. Essas tecnologias não apenas respondem às demandas imediatas, mas moldam ativamente as preferências dos usuários, criando uma simbiose entre humanos e máquinas.

O autor Zampier, ao citar uma pesquisa feita com tomadores de decisão tecnológica informacional, destacou que "87% (oitenta e sete por cento) acreditam que as ferramentas movidas por IA devem estar sujeitas a regulação" (Zampier Lacerda, 2022, p.115)[1]. Informa, ainda, Zampier, com base na referida pesquisa, que seriam necessários quatro pilares a fim de se garantir a governança esperada dos algoritmos artificiais, quais sejam:

[1] O autor é mais conhecido como Bruno Zampier, mas em atenção às regras da ABNT e conforme consta no currículo lattes do autor, preferiu-se colocar Zampier Lacerda.

> 1. integridade: integridade do algoritmo e validade dos dados, incluindo linhagem e adequação de como os dados são usados;
> 2. explicabilidade: transparência por meio do entendimento do processo de tomada de decisão algorítmica em termos de negócios simples;
> 3. equidade: a fim de assegurar que os sistemas de IA sejam éticos, isentos de preconceitos e que os atributos protegidos não sejam usados;
> 4. resiliência: robustez técnica e cumprimento da IA e sua agilidade (Zampier Lacerda, 2022, p. 115).

Enquanto a virtualização sugere uma força vital intrínseca, a digitalização se vincula às Tecnologias da Informação e Comunicação (TICs). Estas, compreendendo infraestruturas de software e hardware, processam dados digitais e fundamentam as tecnologias digitais. No entanto, o estudo realizado pela pesquisa supracitada destaca a algoritmização como termo-chave para a compreensão do atual cenário permeado pela crescente utilização da inteligência artificial. Esta perspectiva ressalta a importância do aprendizado de máquina, evidenciando sua centralidade na aplicação prática da IA, apesar da falta de uniformidade no entendimento do termo (Sarlet, 2022).

Desse modo, a interseção entre algoritmos e inteligência artificial redefine o modo como interagimos com a tecnologia. À medida que algoritmos permeiam o tecido da sociedade digital, a compreensão de sua natureza e da IA torna-se importante. A capacidade de extrair padrões comportamentais, personalizar experiências e moldar a interação humano-máquina delineia um futuro onde a tecnologia não apenas serve, mas coevolui com a humanidade. A algoritmização emerge como a lente pela qual podemos vislumbrar e compreender a complexidade e o potencial transformador dessa jornada tecnológica incessante.

O advento da era tecnológica trouxe consigo uma revolução incessante, impulsionada por algoritmos cada vez mais sofisticados. Estes, por definição, representam conjuntos de regras e instruções que orientam cálculos e processos de resolução de problemas, proporcionando resultados específicos quando ativados. Paralelamente, a inteligência artificial surge como um campo de estudo dedicado ao desenvolvimento de sistemas que reproduzem características e habilidades associadas à inteligência humana (Doneda; *et al*., 2018).

A *Organisation for Economic Cooperation and Development (OECD)* - Conselho da Organização para a Cooperação e Desenvolvimento Econômico (OCDE) aprovou recentemente, em 8 de novembro, a nova definição de Inteligência Artificial, destinada a ser incorporada no novo conjunto de regulamentações de IA da União Europeia. Essa definição foi oficialmente atualizada e provavelmente será integrada no próximo regulamento da UE sobre IA sendo um aspecto de relevante valor para a futura legislação definir seu escopo

(Chatterie; Kern, 2023).

A OCDE, originalmente estabelecida para administrar o Plano Marshall, o pacote de estímulo dos Estados Unidos para financiar a reconstrução da Europa pós-Segunda Guerra Mundial, continua a ser um fórum internacional de cooperação econômica com 38 países membros. Em 2019, a organização propôs um conjunto influente de princípios[2] para políticas confiáveis de IA incluindo uma definição inicial de Inteligência Artificial (Chatterie; Kern, 2023).

A nova definição pela OCDE, como já citado na introdução desta dissertação, estabelece que um sistema de IA é uma máquina baseada em máquina que, para objetivos explícitos ou implícitos, infere, a partir das informações recebidas, como gerar resultados, como previsões, conteúdos, recomendações ou decisões que podem influenciar ambientes físicos ou virtuais. Diferentes sistemas de IA variam em seus níveis de autonomia e adaptabilidade após a implantação. Esta definição foi discutida em meados de outubro de 2023 no Comitê de Política da Economia Digital e no Grupo de Trabalho sobre Governação da Inteligência Artificial da OCDE, com o cronograma ajustado para informar a Lei de IA da UE.

Em março de 2023, a União Europeia concordou em adotar a definição da OCDE para manter a coesão semântica com parceiros internacionais. No entanto, os legisladores enfrentaram a incerteza de que a OCDE atualizaria sua definição com base na evolução tecnológica e de mercado. Na última fase do processo legislativo da Lei de IA da UE, os trílogos, onde a Comissão, o Conselho e o Parlamento da UE discutem as disposições finais, os políticos decidiram aguardar a decisão final da OCDE sobre a definição (Chatterie; Kern, 2023).

A atualização do conceito, conforme observado em uma apresentação conjunta, visa a alinhar internacionalmente as definições de IA, a refletir os desenvolvimentos recentes, melhorar a precisão e a clareza técnica, tornando-a mais preparada para o futuro. Inclui a consideração da inferência na geração de resultados e a expansão das saídas de IA para conteúdo, tal como texto, vídeos ou imagens.

A versão atualizada da definição foi divulgada, e uma das mudanças-chave é a eliminação da condição de que os objetivos devem ser estabelecidos pelo ser humano. Isso possibilita que o sistema de IA aprenda novos objetivos, podendo ser ajustados com feedback do usuário durante a operação, semelhante aos modelos fundamentais.

[2] Princípios baseados nos valores: crescimento inclusivo, desenvolvimento sustentável e bem-estar; centrados no ser humano, na justiça, transparência e explicabilidade, robustez, segurança, proteção e responsabilidade. Disponível em: https://oecd.ai/en/ai-principles.

1.2 TIPOS DE INTELIGÊNCIA ARTIFICIAL, APRENDIZADO DAS MÁQUINAS E ROBÔS

A inteligência artificial é um vasto campo que se desdobra em diversas abordagens, cada uma apresentando nuances distintas em termos de complexidade e autonomia. Entre os tipos de IA mais conhecidos destacam-se a Artificial Narrow Intelligence (ANI) - IA restrita ou também chamada de IA fraca; a Artificial General Intelligence (AGI) - IA geral ou forte, e a Artificial Super Intelligence (ASI) – superinteligência ou Super IA (SIA) (Strelkova; Pasichnyk, 2019). Há quem cite também a existência da IA simbólica, a IA sub-simbólica, e a IA baseada em regras (Zendesk, 2023), cada uma carregando consigo implicações específicas para a responsabilidade civil em casos de danos decorrentes de suas aplicações (Doneda; *et al*., 2018).

A IA restrita (fraca) é caracterizada por sistemas especializados que se concentram em uma área específica e tem um único objetivo definido, como máquinas treinadas para jogar xadrez ou dispositivos eletrônicos domésticos. O autor Bruno Zampier destaca que esta inteligência pode ser dividida em duas subcategorias:

> a) máquinas reativas, uma classe mais simples de sistemas de IA, sem capacidade para gerar acúmulo de memórias e nem observar experiências anteriores para fins de tomada de decisão futura;
> b) memória limitada, em que as máquinas conseguem visualizar e memorizar os fatos passados, com a finalidade de adoção de uma decisão no presente. (Zampier Lacerda, 2022, p. 26).

Assim, a IA restrita contrasta com a IA geral (forte), pois esta é capaz de emular a inteligência humana em diversas áreas e possui diversas habilidades de maneira abrangente, como planejamento, resolução de problemas, pensamento abstrato, compreensão de conceitos complexos e aprendizado rápido por meio da experiência, equiparando-se ao raciocínio humano (Zampier Lacerda, 2022). Comporta também duas ramificações:

> a) máquinas cientes, uma categoria de máquinas que percebem sujeitos à sua volta, objetos e consideram que estes podem ter sentimentos e emoções próprios, ou seja, teriam capacidade de perceber seu entorno. Esta habilidade é tida como essencial para que possam ser estabelecidas relações sociais.
> b) máquinas autoconscientes, que iriam além da consciência sobre o exterior, possuindo até consciência sobre si mesmas, conhecendo e decifrando seus sentimentos interiores. (Zampier Lacerda, 2022, p. 26)

Por sua vez, o conceito de Artificial Super Intelligence (ASI), ou superinteligência, geralmente está associado à ideia de inteligência artificial que ultrapassa a capacidade humana em todas as áreas cognitivas. Superinteligência implica um nível de inteligência tão avançado

que poderia superar as habilidades intelectuais de qualquer ser humano, incluindo habilidades sociais, raciocínio, discernimento e conhecimento geral, embora essa ideia permaneça atualmente limitada ao domínio da ficção científica. Segundo Bruno Zampier, a superinteligência “envolveria desde um computador um pouco mais inteligente que uma pessoa, até aqueles que alcançariam centenas ou milhares de vezes a inteligência humana” (Zampier Lacerda, 2022, p. 27).

Enquanto a IA simbólica utiliza símbolos para representar conhecimento e raciocínio, a IA sub-simbólica opera com dados mais brutos, buscando padrões sem necessariamente compreender o significado por trás deles. A IA baseada em regras, por sua vez, utiliza conjuntos de instruções lógicas para tomar decisões (Doneda, *et al.,* 2018).

Conceituados os tipos de inteligência artificial, tem-se que a inteligência não natural frequentemente utiliza algoritmos, os quais podem ser entendidos como uma sequência de passos empregada pela inteligência artificial para resolver problemas ou executar tarefas, analisando dados e estabelecendo correlações em busca de padrões (Doneda, *et al*., 2018).

Esses algoritmos, por sua vez, podem operar por meio de aprendizado de máquina, que consiste na capacidade da máquina de aprender (*machine learning*) novas informações através da análise de dados e experiências passadas, sem a necessidade de programação explícita, adaptando-se assim a novas situações. O aprendizado profundo, ou *deep learning*, é uma forma avançada de aprendizado de máquina que possui a habilidade de processar diversos tipos de dados de forma similar ao cérebro humano (Doneda, *et al*., 2018).

A interseção entre a complexidade crescente dos sistemas de inteligência artificial, impulsionada pelos modelos de *machine learning* e a fluidez conceitual dessas tecnologias é um tema relevante nos debates contemporâneos. Dessa forma, a profundidade do aprendizado de máquina é explorada por diferentes perspectivas teóricas.

Matthias (2004) destaca a expansão exponencial dessa complexidade, destacando a capacidade das máquinas de adquirirem aprendizado a partir de suas próprias experiências. Smith (2017), por sua vez, oferece uma definição direta do aprendizado de máquina como um processo no qual dados são fornecidos aos computadores, capacitando-os a aprender sem programação explícita. Em termos simples, o aprendizado de máquina proporciona às máquinas a capacidade de "pensar" por si mesmas.

Um exemplo elucidativo é a classificação de imagens através de algoritmos de m*achine learning* que se baseiam em redes neurais convolucionais. Essa abordagem específica emprega uma estrutura de neurônios artificiais projetada para processar informações visuais. Ao adentrar no cerne desse exemplo prático, percebe-se que a

complexidade da classificação de imagens não se resume apenas à execução de tarefas visuais, mas também à capacidade de discernir e interpretar padrões visuais de maneira análoga à cognição humana (Matthias, 2004).

Dessa forma, o processo de aprendizado por máquinas, *machine learning*, permite aos sistemas aprenderem padrões a partir de dados, sem serem explicitamente programados. Outro exemplo que pode ser citado são os algoritmos de *machine learning* utilizados por assistentes virtuais como Siri e *Google Assistant.* Esses assistentes virtuais usam reconhecimento de fala para interpretar comandos de voz a partir da análise de grandes conjuntos de dados de áudio a fim de identificar padrões e aprender a reconhecer palavras e frases (Zampier Lacerda, 2022).

Ainda, se pode mencionar a presença de *machine learning* nas plataformas como Amazon e Netflix que fazem uso dos algoritmos de recomendação para personalizar sugestões de produtos e conteúdo. Tais sistemas de recomendação aprendem com o comportamento passado do usuário e o de outros usuários para sugerir produtos novos (Pires; Silva, 2017).

Os pesquisadores Russel e Norvig (2013) identificam duas características fundamentais da inteligência artificial: o processo de raciocínio e motivação, e o comportamento. A distinção principal reside na habilidade da IA em acumular experiências próprias e aprender com elas, assemelhando-se ao aprendizado autodidata humano. Ademais, complementam a definição, apontando três razões fundamentais para a adoção do aprendizado de máquina. Primeiramente, a incapacidade dos projetistas em antecipar todos os possíveis cenários aos quais o agente pode ser exposto. Em segundo lugar, a impossibilidade de prever as mudanças ao longo do tempo em um ambiente dinâmico. Por fim, em situações específicas, como o reconhecimento de imagens, é inviável criar um algoritmo tradicional que execute a tarefa adequadamente (Russel; Norvig, 2013).

Analisados os tipos de IA, pode-se dizer que robôs são sistemas físicos tecnológicos que realizam tarefas no mundo real. Eles são construídos e programados para desenvolverem uma grande variedade de atividades, como montagem de peças em uma linha de produção, ajudar nas tarefas domésticas e até mesmo servir para exploração espacial.

Alguns dos mais conhecidos robôs estão o robô Kuka, amplamente usado na indústria automobilística, o Roomba, um robô aspirador de pó da iRobot, que navega autonomamente pela casa, limpando o chão e evitando obstáculos, o Curiosity Rover da NASA, que explora a superfície de Marte, entre outros. Há ainda robôs humanoides como o Asimo (Advanced Step in Innovative Mobility) da Honda ou o Sophia da Hanson Robotics, projetados para se parecerem e agirem de maneira semelhante aos humanos, podendo realizar tarefas como receber clientes, fornecer informações e participar de pesquisas sobre interação humano-robô

Vidal, 2024). Além dos cirurgiões robôs que serão analisados em tópico seguinte.

Dessa maneira, os robôs têm a capacidade de operar de forma independente ou serem comandados à distância por pessoas, e uma grande parcela dos robôs atuais integra diferentes aspectos de inteligência artificial, aprimorando assim sua autonomia e habilidade decisória. Por outro lado, a IA, como já analisado anteriormente, são sistemas ou máquinas que imitam a inteligência humana para realizar tarefas e podem se aprimorar com base nas informações que coletam, por meio do aprendizado de máquina ou aprendizado profundo (*deep learning*).

Assim, quando um robô utiliza sistemas de IA para realizar suas tarefas de maneira autônoma, ele pode ser considerado um tipo de IA. No entanto, nem todos os robôs têm IA, alguns operam com base em conjuntos de instruções pré-programadas simples e não têm a capacidade de aprender ou adaptar-se a novas situações. Da mesma forma, nem toda IA está em um robô, muitas operam puramente em ambientes digitais, como assistentes virtuais, sistemas de recomendação ou motores de busca.

A compreensão clara e transparente do funcionamento desses modelos, não apenas é fundamental para evitar danos, mas também para estabelecer critérios éticos e legais na aplicação da inteligência artificial em diversas esferas da sociedade. Nesse aspecto, para melhor estudar o tema proposto no presente trabalho, é importante compreender os robôs inteligentes utilizados na área médica, como será feito no item a seguir.

1.3 AVANÇOS DA INTELIGÊNCIA ARTIFICIAL NA MEDICINA: O IMPACTO TRANSFORMADOR DOS ROBÔS CIRÚRGICOS

Em 2004, a Agência de Projetos de Pesquisa Avançada de Defesa dos Estados Unidos – *Defense Advanced Research Projects Agency* (DARPA) lançou um desafio com recompensa de um milhão de dólares para o desenvolvimento de um veículo autônomo capaz de atravessar 230 km de terreno irregular, ligando Barstow, na Califórnia, a Primm, em Nevada. Mais de uma década depois, em 2017, o Departamento de Defesa dos Estados Unidos introduziu um novo desafio, focado na criação de médicos robóticos autônomos, marcando um avanço significativo na intersecção da tecnologia e da medicina (Gaines, 2022).

Os robôs cirúrgicos, desde sua concepção até a atualidade, prenunciam um futuro brilhante marcado pela inovação contínua. A sinergia entre cirurgiões e robôs, reforçada pela inteligência artificial, promete redefinir a cirurgia moderna, indicando uma revolução iminente que merece atenção detalhada. A aplicação de conceitos modernos como assistência computacional, automação e realidade virtual à medicina ampliou os benefícios da cirurgia

robótica, como aprimoramento da visualização, precisão e destreza. Com mais de três décadas de presença na medicina, os robôs cirúrgicos estabeleceram um novo padrão de cuidados, destacando-se por sua capacidade de realizar atividades físicas e interagir de forma mais direta com a realidade.

O termo robô cirúrgico refere-se a qualquer dispositivo eletromecânico que executa funções cirúrgicas, incluindo cortar, cauterizar e suturar tecidos, sem feedback mecânico direto para um operador humano (Morrell; *et al*, 2021). O conceito geral de um robô cirúrgico abrange sistema computacional que executa funções cirúrgicas sob o controle de um cirurgião. Esta definição enfatiza a capacidade do robô de realizar procedimentos cirúrgicos de forma autônoma, ou seja, sem intervenção direta durante a operação, o que potencialmente aumenta a precisão e reduz riscos associados à intervenção humana direta. Esses robôs oferecem precisão aumentada, movimentos mais refinados e a capacidade de realizar tarefas cirúrgicas com menos fadiga e maior ergonomia para o cirurgião (Nogaroli, 2021).

Desde a década de 1980, a robótica tem sido uma presença constante em salas cirúrgicas, inicialmente servindo como auxiliares que mantinham em posição os membros dos pacientes durante procedimentos. Com o passar dos anos, essa tecnologia evoluiu para a cirurgia laparoscópica, permitindo que médicos realizassem operações através de incisões mínimas, com o auxílio de braços robóticos operados à distância, em vez de grandes cortes (Gaines, 2022).

Corroborando, no ano de 2008, aconteceu no Brasil a primeira cirurgia por meio de robô cirúrgico, e desde então, o número de robôs cirúrgicos no Brasil aumentou para 41, enquanto em 2008 existiam menos de dezoito. Assim, o número desses procedimentos vem aumentando de forma constante, abrangendo diversas especialidades cirúrgicas. Desde esse período, mais de 17 mil procedimentos cirúrgicos robóticos foram realizados, com o Hospital Israelita Albert Einstein em São Paulo liderando a inovação (Nogaroli, 2021). No Sistema Único de Saúde (SUS), o alto custo dos avanços tecnológicos representa um obstáculo significativo. Adquirir o sistema Da Vinci tem um custo aproximado de 2,5 milhões de dólares, tornando o país dependente do desenvolvimento de tecnologias mais acessíveis. Esse desafio está nas mãos das empresas que projetam e fabricam esses robôs cirúrgicos (Nogaroli, 2023).

No entanto, a visão de um cirurgião robótico totalmente independente ainda enfrenta grandes desafios, não apenas tecnológicos, mas também na aceitação pública de sua segurança e eficácia (Gaines, 2022). Ainda, especula-se que métodos robóticos autônomos e semiautônomos se tornarão aceitos como uma modalidade padrão e, assim, revolucionarão a

cirurgia. Esses robôs autônomos formarão um elemento essencial da tecnologia de ponta. Capacidades aprimoradas de *machine learning* podem habilitar cirurgiões virtuais robóticos autônomos e lançar a próxima geração de IA (O'Sullivan, *et al*., 2019). Vale investigar se isso poderia ser comparável à inteligência e consciência de nível humano do "Teste de Turing". Enquanto isso, técnicas existentes anunciarão as primeiras quatro gerações (1ª—Estereotáxica; 2ª—Endoscópica; 3ª—Bioinspirada; 4ª—Microbots) de robôs cirúrgicos utilizando capacidade de decisão autônoma adicionada (5ª geração), mesmo que aquém de uma IA totalmente geral (O'Sullivan; *et al*, 2019).

Resultados tão positivos confirmam o potencial para robôs autônomos, mostrando-se capazes de melhorar a eficácia, consistência, resultado funcional e a viabilidade de implementação de técnicas cirúrgicas (O'Sullivan; *et al*., 2019). Entretanto, a cirurgia robótica autônoma enfrenta limitações, como a variabilidade da anatomia humana e situações inesperadas, além das capacidades de percepção e feedback dos robôs, que podem comprometer a tomada de decisões precisas. Outros desafios incluem os custos associados ao desenvolvimento, aquisição e implementação dessas tecnologias, limitando sua disponibilidade e acessibilidade (Nogaroli, 2023).

1.3.1 Robôs Cirúrgicos: Até Da Vinci evolução dos robôs cirúrgicos

A jornada evolutiva dos robôs cirúrgicos, iniciada na década de 1920 com a cunhagem do termo "robô" por Karel Čapek, reflete um marco histórico que transcende as convenções tradicionais. Originado do termo tcheco "robota", que significa "trabalho forçado", o conceito inicial de robô era associado a tarefas repetitivas realizadas por máquinas desprovidas de inteligência artificial. No entanto, a moderna definição de robôs, identifica três atributos fundamentais: a capacidade de responder a estímulos através de sensores, a governança por algoritmos que determinam suas ações, e a habilidade de intervir no mundo exterior de forma significativa (Froomkin, 2016).

Eventos notáveis como a Operação Lindberg, que permitiu cirurgias transatlânticas, e o desenvolvimento de sistemas como o Da Vinci XI, evidenciam a ascensão constante da tecnologia robótica. Desafiando a predominância do sistema Da Vinci, novas plataformas como o SPORT da Titan Medical e o Versius® da Cambridge Medical Robotics introduzem no mercado opções com maior flexibilidade operacional (Morrell; *et al*, 2021).

A genealogia da cirurgia robótica remonta ao Programmable Universal Machine for Assembly (PUMA) 560, que seria uma máquina robótica com seis graus de liberdade

utilizado pela primeira vez por Kwoh e colaboradores, em 1985, para biópsias neurocirúrgicas com uma precisão notavelmente alta. Essa inovação foi seguida pela adoção do sistema PROBOT em 1988, através de uma resseção transuretral da próstata. Posteriormente, o desenvolvimento do ROBODOC Surgical System em 1992 pela empresa Integrated Surgical Supplies, sendo o primeiro a receber aprovação da FDA (Food and Drug Administration) nos Estados Unidos, e voltado para o suporte na inserção de uma prótese total do quadril mais eficaz (Dasgupta; IS, 2005).

A década de 1990 testemunhou avanços significativos com a fundação da *Computer Motion* por Yulun Wang e o desenvolvimento do sistema AESOP, que melhorou a estabilidade das imagens cirúrgicas e reduziu a necessidade de assistência médica. Em 1998, a Alemanha viu a primeira utilização do robô Da Vinci, facilitando cirurgias cardíacas complexas. Em 2000, a aprovação pela FDA deste sistema para cirurgia geral marcou a aceitação e expansão dessa tecnologia transformadora (Morrell; *et al.*, 2021).

Destarte, a história do desenvolvimento da cirurgia robótica autônoma tem sido marcada por avanços significativos, desde o uso do primeiro robô cirúrgico para biópsias neurocerebrais até a aprovação do sistema Da Vinci para cirurgia geral (sistemas semelhantes incluem Mako, ROBODOC, CyberKnife ou Renaissance, e empresas de cirurgia robótica de destaque incluem Intuitive Surgical, Smith & Nephew, Stryker, Mazor Robotics, Zimmer Biomet). A autonomia na cirurgia robótica é categorizada em diferentes níveis, destacando a transição do controle do humano para a máquina e a capacidade do robô de adaptar-se a novas situações.

Em termos de métodos robóticos autônomos, o mais conhecido é robô de anastomose de tecido inteligente (conhecido como STAR). Este é o conceito de prova para um sistema cirúrgico robótico guiado por visão. O sistema utiliza uma ferramenta de sutura laparoscópica acionada que implementa comandos baseados em imagem para realizar tarefas especificadas. Ele superou cirurgiões humanos em sutura laparoscópica, exibindo maior precisão, consistência e velocidade. Eles demonstraram ainda que o procedimento autônomo supervisionado pelo STAR é superior à cirurgia realizada por cirurgiões especialistas (Morrell; *et al*.,2021).

Nesse contexto, cabe destaque a adoção do robô Da Vinci, fabricado pela Intuitive Surgical, uma empresa norte-americana. Desde o ano 2000, cerca de seis milhões de procedimentos cirúrgicos foram realizados globalmente com a assistência deste robô, evidenciando um aumento notável no número de cirurgias robóticas. Somente nos Estados Unidos, a quantidade de cirurgias realizadas com a ajuda de robôs saltou de aproximadamente

136 mil em 2008 para 877 mil em 2017, segundo informações da Intuitive Surgical (Surgical, 2024).

O robô Da Vinci oferece uma precisão sem precedentes em cortes e suturas, graças à flexibilidade dos seus punhos robóticos que podem girar 360º e à capacidade de eliminar os tremores naturais das mãos humanas. Tais avanços tecnológicos trouxeram benefícios consideráveis, incluindo redução da perda de sangue durante as cirurgias, menores cicatrizes, diminuição da dor, menor necessidade de medicação pós-operatória e recuperação mais rápida dos pacientes (Nogaroli, 2023).

O sistema Da Vinci é rotineiramente usado para operações como cirurgia renal, cirurgia urogenital, cirurgia cardíaca, cirurgia de cólon e prostatectomias, embora muitos outros procedimentos estejam atualmente em desenvolvimento. Atualmente, muitos assumem que há aprovação para cirurgia assistida por robô que requer telepresença humana. (Morrell; *et. al.*, 2021). Nos EUA, e de maneira similar na Europa e em outros lugares, o robô cirúrgico da Vinci é aprovado para uso em humanos vivos, mas esse robô é completamente controlado por um cirurgião altamente qualificado e especialmente treinado. O cirurgião fica na mesma sala onde o robô opera, e a qualquer momento, se algo der errado com o procedimento robótico, o cirurgião pode voltar para um procedimento aberto tradicional (Nogaroli, 2023).

Contudo, a adoção dessas tecnologias não está isenta de riscos. Entre 2000 e 2013, foram reportados 10.624 eventos adversos nos Estados Unidos relacionados ao uso do robô Da Vinci, incluindo 144 mortes, 1.391 lesões em pacientes e 8.061 falhas de dispositivos, conforme um estudo retrospectivo sobre dados da FDA (Nogaroli, 2023).

Entre os benefícios da cirurgia robótica, destacam-se a alta definição, visão estereoscópica tridimensional com ampliação, câmera estável controlada pelo cirurgião, melhor ergonomia e uma gama ampliada de movimentos e precisão. Entretanto, o sucesso desses procedimentos não se deve apenas ao robô, mas ao sistema integrado de infraestrutura e ao contínuo treinamento de médicos e enfermeiros, essencial para alcançar resultados altamente positivos (Nogaroli, 2023).

A inteligência artificial e a aprendizagem profunda desempenham papéis fundamentais nesta evolução, permitindo a máquinas operadas por IA auxiliar no planejamento pré-operatório e na visualização da anatomia do paciente, o que, por sua vez, melhora a precisão cirúrgica, segurança e treinamento. Este avanço segue o padrão das curvas S tradicionais, indicando uma fase de inovação tecnológica seguida por uma vantagem de desempenho sobre os padrões atuais, antes de atingir um platô de desempenho (Morrell; *et al.,* 2021).

Assim, desde suas origens até os dias atuais, os robôs cirúrgicos se consolidaram como

um dos avanços mais significativos na medicina, oferecendo procedimentos com maior precisão e resultados otimizados para os pacientes. Esta evolução não apenas reflete o progresso técnico e tecnológico dos robôs, mas também uma mudança paradigmática na prática cirúrgica, sublinhando o imenso potencial da integração entre tecnologia e saúde.

2 IMPLICAÇÕES JURÍDICAS DO EMPREGO DE INTELIGÊNCIA ARTIFICIAL E A RESPONSABILIDADE CIVIL

Analisada a evolução dos robôs cirurgiões, este capítulo examina as complexas implicações jurídicas decorrentes do uso crescente de inteligência artificial (IA) e sua subsequente relação com a responsabilidade civil. Em uma era marcada por avanços tecnológicos acelerados, a integração da IA em diversos setores levanta questões críticas sobre *accountability*, direitos e deveres legais.

A análise é enriquecida com as contribuições de Rosenvald e Braga Netto (2024), cujas perspectivas sobre a responsabilidade civil fornecem uma base teórica sólida para nosso estudo. No entanto, para abordar a multifaceticidade do tema, este capítulo também incorpora *insights* de outros renomados estudiosos. Exploramos, por exemplo, as opiniões divergentes sobre a capacidade de agência da IA e suas implicações para os princípios tradicionais de culpa e responsabilidade. Através de uma revisão literária abrangente e uma análise crítica, buscamos entender como as legislações atuais podem evoluir para melhor regulamentar essa nova realidade, equilibrando inovação tecnológica com proteção legal e ética adequadas.

2.1 EXPLORANDO OS CONCEITOS DA RESPONSABILIDADE CIVIL NA ERA DAS NOVAS TECNOLOGIAS

A partir da invasão tecnológica, experimentada de forma contundente há alguns anos, a transmutação das ações outrora encontradas na sociedade para um mundo digital cada vez mais aceito e consolidado, tem suscitado dúvidas consistentes acerca da estrutura normativa disposta no ordenamento jurídico atual. A busca por adequações urgentes dos novos formatos digitais, que tendem a dominar as relações interpessoais cada vez mais globalizadas, apontam não apenas no sentido do desenvolvimento de legislação específica, capaz de acomodar as inovações tecnológicas e suas peculiaridades, mas ainda na ressignificação de normas (princípios e regras) já existentes, assim como na percepção do particular como protagonista em meio ao sistema jurídico.

Dessa forma, o desenvolvimento e o avanço tecnológico têm transformado profundamente a maneira como as pessoas vivem, trabalham e interagem com o mundo ao seu redor. Os sistemas inteligentes permitem personalizar produtos, serviços e experiências com base nas preferências e histórico dos usuários. Isso cria interações mais relevantes e satisfatórias, como recomendações personalizadas, assistentes virtuais e *chatbots*. Essas

mudanças têm exposto a pessoa a uma série de desafios nunca antes imaginados. De forma ainda mais sensível, haverá prejuízos de ordem existencial ao ser humano.

Isso porque, o cenário tecnológico disruptivo que caracteriza o presente abala o antropocentrismo que é a base do direito privado. Isso fica evidente por meio de movimentos que desafiam a premissa humanística do ramo civilista. Segundo Arendt (2005), o que atualmente denominamos como privacidade constitui um círculo íntimo cujas raízes podem ser rastreadas até os últimos estágios da civilização romana, mas cujas características distintas, diversidade e complexidade eram indubitavelmente sem precedentes em qualquer época que antecedesse a era moderna.

Nessa conjuntura, as relações entre o público e o privado passaram por transformações significativas. Por um lado, a presença de outros que compartilham nossa visão e percepção é essencial para assegurar a realidade do mundo e de nossa própria existência. No entanto, por outro lado, a profundidade da vida privada plenamente desenvolvida amplifica e enriquece consideravelmente o espectro das emoções subjetivas e dos sentimentos pessoais. Essa intensificação, todavia, ocorre frequentemente à custa da segurança na certeza do mundo exterior (Arendt, 2005).

A responsabilidade civil no século XXI deve ser abordada de maneira inovadora e contemporânea, considerando ideias frescas e renovadas. A complexidade substancial do sistema jurídico, especialmente com a ascensão do neoconstitucionalismo, demanda que o intérprete examine os padrões de atuação dos setores privados à luz dos princípios constitucionais, integrando-os aos paradigmas tradicionais de interpretação jurídica. Para explorar as novas perspectivas da responsabilidade civil, é essencial, portanto, começar com uma abordagem do direito civil constitucional.

O direito civil, sob uma perspectiva constitucional, coloca o indivíduo como o ator central no sistema jurídico, onde bens e serviços são concebidos para servir às pessoas. O ser humano assume o papel de protagonista, com grande destaque na proteção e garantia de direitos (Rosenvald; Braga Netto, 2024). No entanto, é notável que, nos dias atuais, algumas das premissas fundamentais do direito civil constitucional, que valorizam o papel do ser humano, estão sendo desafiadas pelo fenômeno denominado por Nelson Rosenvald como a 'despersonalização do direito da personalidade' (Rosenvald; Braga Netto, 2024).

O uso de dados pessoais, para alimentar os novos sistemas de inteligência artificial e tomar decisões, está resultando em uma precisão significativa em várias aplicações. Isso levanta dois temas essenciais para futuros debates sobre autonomia e direitos fundamentais. Em primeiro lugar, é importante considerar os efeitos que o uso desses sistemas terá nas

pessoas e em sua autonomia pessoal. Em segundo lugar, é necessário definir a natureza dessas ferramentas e sistemas de inteligência artificial (Doneda; *et al*., 2018).

Nesse contexto, é imperativo encontrar soluções que protejam os direitos fundamentais, especialmente em um cenário de rápido avanço tecnológico e questionamento de conceitos jurídicos fundamentais. Isso sugere a importância de recorrer à ética como uma ferramenta para orientar possíveis soluções, que eventualmente poderiam se traduzir em medidas legislativas para o futuro (Doneda *et al*., 2018). Primeiramente, há a 'expropriação da personalidade,' que se refere ao fato de que a realidade digital transforma as experiências existenciais em uma nova realidade digitalizada, uma nova forma de propriedade. Essa digitalização muitas vezes envolve a apropriação não autorizada daquilo que nos define como indivíduos (Rosenvald; Braga Netto, 2024).

Conforme discutido pela autora Shoshana Zuboff (2019) em seu livro 'Capitalismo de Vigilância', a atual era do capitalismo de vigilância não se resume a uma nova tecnologia, mas sim a um modelo de mercado em que a experiência humana é unilateralmente reivindicada como matéria- prima gratuita. Isso porque, segundo discorre a autora, estamos vivendo em uma era em que as empresas, especialmente as gigantes da tecnologia, estão coletando dados pessoais em grande escala, por meio de dispositivos, aplicativos e serviços digitais, como exemplo informações sobre nossos hábitos de navegação na internet, localização, histórico de compras, comunicações e muito mais. (Zuboff, 2019).

Essa experiência é traduzida em dados, que podem ser usados para segmentar anúncios de forma altamente direcionada, influenciar comportamentos de compra e criar produtos e serviços personalizados, que são comercializados como produtos de previsão que moldam e antecipam comportamentos humanos futuros e controle social. Assim, como defendido por Zuboff (2019), o chamado capitalismo de vigilância mina os fundamentos antropocêntricos do direito civil, reivindicando unilateralmente a experiência humana como matéria-prima gratuita para traduzi-la em dados comportamentais. Esses dados são então disponibilizados no mercado como produtos de predição e influenciam comportamentos futuros.

Dessa forma, o capitalismo de vigilância não se limita apenas à coleta de dados, mas também envolve o uso desses dados para influenciar o comportamento das pessoas. Isso pode ser feito por meio de anúncios direcionados, manipulação de conteúdo em *feeds* de notícias e algoritmos que determinam o que vemos na internet.

Caso Immanuel Kant, o filósofo do Iluminismo, contemplasse essa disposição moderna, provavelmente a consideraria uma subversão da ideia de que o ser humano é um fim

em si mesmo. Nesse novo contexto, o ser humano é frequentemente instrumentalizado, e, em última instância, sua personalidade pode ser usurpada em prol de interesses alheios. A própria sociedade se torna um objeto de controle para fins diversos (Rosenvald; Braga Netto, 2024).

Além disso, outro movimento significativo que está ocorrendo nos dias atuais é a ameaça à autonomia individual por meio de ataques à nossa consciência. Muitas vezes, os usuários não têm plena consciência de como seus dados estão sendo coletados e usados, e podem não ter controle real sobre o processo. A falta de transparência e consentimento informado é uma preocupação fundamental (Rosenvald; Braga Netto, 2024).

No contexto do Direito Civil, a autonomia privada é tradicionalmente considerada a pedra angular do civilismo. Ela se refere à capacidade das pessoas de autodeterminação, não apenas em questões contratuais e econômicas, como contratar e possuir propriedades, mas também em relação à gestão de seus próprios pensamentos, emoções e desejos. No entanto, com os avanços tecnológicos da era atual, a base filosófica subjacente à autonomia privada, que se baseia na noção de livre arbítrio, tem passado por transformações profundas (Rosenvald; Braga Netto, 2024).

Ainda, para os autores supracitados, os neurocientistas, físicos e pesquisadores têm argumentado que, na verdade, existe um determinismo subjacente às ações humanas. A ideia de livre arbítrio é muitas vezes considerada uma ilusão na era da narrativa neoliberal. De acordo com essa perspectiva, os seres humanos são, em última instância, apenas conjuntos de conexões químicas e elétricas em seus cérebros (Rosenvald; Braga Netto, 2024).

A ideia de que o ser humano é um conjunto de algoritmos é uma perspectiva que desafia a concepção tradicional da natureza humana, especialmente, no contexto das ciências cognitivas, da filosofia da mente e da inteligência artificial. Essa perspectiva sugere que os processos mentais, comportamentais e cognitivos que caracterizam os seres humanos podem ser entendidos e explicados por meio de algoritmos computacionais, semelhantes aos usados em sistemas de inteligência artificial. Isso implica que, dadas as mesmas entradas (informações) e as mesmas condições iniciais, as respostas ou ações de um ser humano seriam previsíveis, como as saídas de um algoritmo (Doneda, *et al*, 2018).

Tal perspectiva é muitas vezes considerada uma forma de reducionismo, pois busca reduzir a complexidade da mente humana a processos computacionais mais simples. Ela desafia a visão tradicional de que a mente humana é intrinsecamente complexa e não pode ser totalmente compreendida em termos de algoritmos. Dessa forma, muitos cientistas, filósofos e pesquisadores argumentam que a mente humana é muito mais complexa do que qualquer modelo algorítmico atualmente compreendido, e que a experiência humana envolve

aspectos emocionais, subjetivos e sociais que não podem ser reduzidos a meros algoritmos (Rosenvald; Braga Netto, 2024).

Para os autores supracitados, gera debates filosóficos profundos sobre questões como livre arbítrio, moralidade e a natureza da consciência. Afinal, se os seres humanos são apenas algoritmos, isso pode levantar questões sobre a responsabilidade individual e a ética. Caso essa visão prevalecer, ela desafia profundamente a noção de pessoa, que é fundamental para o direito civil, porque, sob essa nova perspectiva, o ser humano é otimizado e tratado como um mero conjunto de algoritmos, passível de manipulação e comercialização (Rosenvald; Braga Netto, 2024).

Esse debate sobre a natureza da autonomia e a ameaça à nossa capacidade de autodeterminação levanta questões importantes sobre como as mudanças tecnológicas estão moldando não apenas o direito civil, mas também a nossa compreensão da natureza humana e da responsabilidade individual. À medida que avançamos no século XXI, é essencial abordar essas questões para garantir que os direitos e a dignidade das pessoas sejam preservados em um mundo cada vez mais digital e interconectado (Rosenvald; Braga Netto, 2024).

O processo de despossessão do Eu pode se manifestar de diversas maneiras, sendo duas delas particularmente relevantes: a dispensa do consentimento e o ataque à nossa consciência. Além das situações já mencionadas, é importante observar como a evolução tecnológica e a crescente presença das *big techs* na nossa vida cotidiana têm desempenhado um papel significativo nesse cenário (Rosenvald; Braga Netto, 2024).

A dispensa do consentimento tornou-se mais evidente com a proliferação dos contratos de adesão on-line. É notável que, ao navegar por um *site* na internet, muitas vezes somos automaticamente obrigados a aceitar os termos de serviço. O que é preocupante é que esses acordos podem ser alterados a qualquer momento, sem a necessidade de consentimento da outra parte contratante. Essa unilateralidade na apropriação de direitos é alarmante e desafia as bases do contrato tradicional.

É importante ressaltar que os termos de uso utilizados pelas gigantes da tecnologia se tornaram uma linguagem comum no direito digital. No entanto, muitas vezes, esses termos de serviço incluem políticas de privacidade que, na realidade, não oferecem nenhuma garantia de privacidade. O acesso aos serviços é frequentemente condicionado ao compartilhamento de dados sensíveis com terceiros, sem que haja uma clara declaração de responsabilidade por parte dessas empresas terceirizadas. Isso representa uma ameaça grave à privacidade e à segurança dos dados pessoais.

Contudo, não é apenas o consentimento do ser humano que está sendo eliminado nesse

processo. A própria consciência individual está sob ataque, graças ao uso de técnicas que visam modificar o comportamento humano. A autonomia, que reside na capacidade de premeditar, fazer escolhas e julgamentos morais, está sendo minada por práticas que manipulam sutilmente nossas decisões (Rosenvald; Braga Netto, 2024).

Um exemplo disso é o que Richard Yonck chamou de "economia da emoção" (Yonck, 2017). Nesse contexto, não somos monitorados apenas pelo conteúdo que consumimos, mas também pela forma como nos expressamos, nossa respiração, tom de voz e outros metadados que revelam nossas características psicológicas e emocionais. Esses dados são usados para criar perfis detalhados que, por sua vez, influenciam as decisões que nos são apresentadas (Rosenvald; Braga Netto, 2024, p. 5).

Curiosamente, um dos primeiros encontros da humanidade com a inteligência artificial foi através das redes sociais, onde a IA muitas vezes age como um curador de conteúdo, selecionando quais sons e imagens chegam até nós. Essa curadoria é frequentemente orientada pelo engajamento, o que cria uma ilusão de escolha e liberdade, mas, na realidade, nos submete a uma cortina de ilusões que distorcem nossa autonomia.

Nesse cenário, o constituinte originário do Brasil estabeleceu de forma precisa o direito fundamental à intimidade e à vida privada no artigo 5º, X, da Constituição Federal de 1988 (Brasil, 1988). Além disso, o poder reformador incorporou expressamente o direito fundamental à proteção de dados pessoais por meio da Emenda Constitucional n.º 115/2022. Dessa forma, as instituições da sociedade civil e a jurisdição constitucional desempenham papéis de destaque.

Um exemplo relevante dessa proteção constitucional foi observado na Ação Direta de Inconstitucionalidade (ADI) n.º 6.649, na qual foi impugnado o Decreto n.º 10.046/2019, que ultrapassou os limites do poder regulamentar da Presidência da República ao promover o compartilhamento e a integração de informações pessoais sem as devidas cautelas. Essa iniciativa foi considerada uma violação direta aos direitos à proteção de dados pessoais, à intimidade e à vida privada das pessoas naturais, e, portanto, foi objeto de questionamento perante a jurisdição constitucional (Robl Filho, 2023).

Essas ações demonstram o comprometimento das instituições brasileiras em salvaguardar os direitos fundamentais relacionados à intimidade, vida privada e proteção de dados pessoais, buscando assegurar o respeito à Constituição Federal e a proteção dos cidadãos em um ambiente cada vez mais digital e conectado.

A despersonalização da individualidade implica na transformação do ser humano em um mero objeto de personalização (Rosenvald; Braga Netto, 2024). Em outras palavras, isso

implica em transformar a vida humana em uma *commodity*, trocando-a por segurança e conveniência. Dessa forma, como mencionado anteriormente, o direito deixa de ser aplicado em prol da pessoa, que deixa de ser a protagonista do sistema jurídico.

Levando em conta todas essas considerações, é fundamental que a responsabilidade civil possua novas perspectivas, dimensões a fim de dar uma resposta a este "estado de coisas". Para tanto, a responsabilidade civil deve ser analisada em outras três funções, além da *liability*, quais sejam: a *responsibility, accountability e answerability*. A *responsibility, accountability e answerability* são termos que vão além da simples função judicial de reparar danos, adicionando novos aspectos à responsabilidade, que são capazes de lidar com a complexidade e a rapidez das estruturas sociais atuais (Faleiros Júnior, 2024).

Em plena era da sociedade da informação, é inadmissível analisar a responsabilidade de forma simplista, apenas através de uma abordagem conceitual básica. Nesse contexto, é fundamental compreender os conceitos de *liability*, *responsibility*, *accountability* e *answerability* para abordar de maneira contemporânea o instituto da responsabilidade civil.

2.1.1 *Liability*

Ultimamente, tem-se observado dentro da comunidade jurídica internacional um crescente reconhecimento da importância da *accountability* na evolução da responsabilidade legal ou estrita tradicional, conhecida na doutrina estrangeira como *liability*, para um modelo de responsabilização que prioriza funções preventivas e precautórias, conforme proposto por Giovanni Comandé (2019). O objetivo é não apenas compensar os danos, mas também prevenir sua ocorrência, introduzindo um sistema mais proativo de responsabilidade civil. Nessa linha, Comandé (2019) destaca a importância de transformar a responsabilidade estrita (*liability*) para uma responsabilidade civil que inclua a função preventiva e precaucional (riscos desconhecidos), impondo aqueles "deveres informados por dados" (data-informed duties) aos desenvolvedores e operadores de IA.

A *liability*, ou responsabilidade legal, é um termo em inglês que se refere à responsabilidade ou obrigação legal de alguém ou de uma entidade, como uma pessoa, uma empresa ou uma organização. É usado para descrever a situação em que alguém é legalmente responsável por suas ações. Assim, refere-se à obrigação legal de reparar danos causados a terceiros em decorrência de uma conduta ilícita. Isso inclui casos em que uma pessoa ou entidade é considerada legalmente responsável por negligência, conduta imprópria ou violação de leis ou regulamentos (Xueting, 2022).

Tradicionalmente, a responsabilidade civil baseia-se na noção de culpa e causalidade, requerendo a demonstração de negligência ou conduta ilícita para atribuição de responsabilidade. Contudo, na era digital, onde sistemas autônomos e algoritmos desempenham papéis significativos, surgem questionamentos sobre como atribuir responsabilidade diante de danos causados por inteligência artificial (Tepedino; Silva, 2019).

Dessa forma, a *liability* pode se estender a desenvolvedores de software, fabricantes de produtos tecnológicos e operadores de sistemas automatizados em casos de falhas de segurança, bugs ou mau funcionamento que resultem em danos a usuários ou outras partes interessadas.

Em sintonia com o pensamento de Nelson Rosenvald (2024), a ideia de *liability* sugere a compensação decorrente da conexão entre a conduta e o dano, sendo influenciada por outros fatores considerados de acordo com a relação direta de atribuição, levando em consideração as particularidades de cada jurisdição. Certamente, a *liability* não é imutável. Em vez de ser a tradicional responsabilidade civil, que é individualista, reativa e centrada no patrimônio, há diferentes demandas sociais gradualmente transformaram os fundamentos da responsabilidade civil. Vamos analisar isso.

A cláusula geral de imputação objetiva presente no artigo 927 do Código Civil, em seu parágrafo único, está vinculada ao princípio da solidariedade, impondo a obrigação de reparação como uma medida de segurança social diante do risco inerente a certas atividades (Braga Netto, 2024). O mero ato de praticar um comportamento ilegal pode ser punido por meio da tutela inibitória quando as circunstâncias assim o indicarem, conforme art. 12, parágrafo único, CC.

Quando uma atividade ou produto apresenta potencial lesivo, ele pode sofrer restrições se a ponderação de bens indicar a necessidade de antecipar riscos. Aqui, o nexo causal transcende a causalidade natural, assumindo uma causalidade puramente jurídica e diluída em situações que merecem tutela. Isso permite a responsabilização em cenários onde há uma vinculação entre um fato e um risco hipotético (Rosenvald; Braga Netto, 2024).

O direito civil, portanto, passou a reconhecer novos tipos de danos além da dicotomia tradicional entre danos patrimoniais e morais. Danos estéticos, danos existenciais e a perda de uma chance são exemplos de novas formas de danos que agora recebem proteção jurídica. Essa evolução mostra uma tendência favorável à multifuncionalidade da responsabilidade civil, adaptando o conceito de *liability* às sociedades altamente tecnológicas em que vivemos (Rosenvald; Braga Netto, 2024).

De maneira geral, percebe-se que essa abordagem moderna de "liability" busca

integrar medidas que assegurem a *responsibility, accountability e answerability* dos envolvidos, exigindo que práticas, rotinas e procedimentos sejam estabelecidos de modo a minimizar riscos e proteger as partes envolvidas antes que qualquer dano ocorra. A mudança reflete uma visão mais holística e sustentável da responsabilidade civil, adequada para lidar com os complexos desafios de um mundo cada vez mais interconectado e tecnológico.

2.1.2 *Responsibility*

A *responsibility*, também é um termo em inglês, e por sua vez, vai além da *liability* e envolve a noção de responsabilidade moral ou ética, pois diz respeito à obrigação ética de agir de maneira adequada e consciente, assumindo as consequências de suas ações. Isso implica assumir a responsabilidade pelas consequências de nossas ações, mesmo que não sejamos legalmente obrigados a fazê-lo.

Segundo Elena Simina Tanasescu, a ideia de *responsibility* está ligada a uma regra ética com status de princípio, semelhante ao da igualdade e da liberdade, e que implica no dever de cuidado com os resultados de suas condutas. Está ligada à capacidade de agir de modo legalmente compatível e tomar decisões conscientes e éticas. (Tanasescu, 2011).

O termo *responsibility* implica no sentido moral da obrigação, sendo assumida voluntariamente e nunca imposta. Trata-se de um conceito possível de responsabilidade, no qual se transforma em uma ferramenta para autodeterminação e um padrão de conduta. Não há diretrizes formais para a *responsibility*, pois as entidades não possuem a capacidade de determinar se uma ação é responsável ou não. Isso é algo que cabe a cada indivíduo decidir diariamente, se interferirá inadequadamente ou não na vida de outras pessoas (Rosenvald; Braga Netto, 2024).

Nesse sentido, como inferem os autores Jos Lehmann *et al*. (2006), a atribuição de *responsibility* pode variar significativamente de pessoa para pessoa. Refletem tais autores que a noção de *responsibility* envolve o problema de quanta influência o senso comum deve ter na determinação e atribuição da responsabilidade legal[3]. Portanto, a atribuição de *responsibility* exige análises detalhadas (e preventivas) sobre os critérios explícitos que devem ser usados

[3]Os autores demonstram dois principais tipos de elementos, que podem desempenhar um papel na atribuição de responsibility: "(1) On the one hand, there are factual elements, which contain information for establishing the chain of causation and which, therefore, make it possible to attribute the responsibility of the harm to the person(s) who caused it.
(2) On the other hand, there are the legal elements of the case, which contain information for identifying the person(s) who may be held responsible for the harm, based on so called considerations of legal policy" (LEHMANN, J., Breuker, J. & Brouwer, B. Causation in AI and Law. Artif Intell Law 12, 279–315. 2004. https://doi.org/10.1007/s10506-005-4157-y. p. 287).

por um juiz ao responsabilizar alguém pelo dano causado a outra pessoa.

É precisamente essa busca por consistência que levanta difíceis questões sobre os critérios de atribuição de *responsibility* (Lehmann *et al*., 2006). Nesse sentido, Hart e Honoré (1985) reduzem a noção de *responsibility* ao status legal de alguém que está sujeito a uma punição ou sanção legal. Assim, *responsibility* é a obrigação de uma pessoa ser punida, forçada a compensar, ou de outra forma sujeita a uma sanção pela lei.

A *responsibility* adota um enfoque preventivo, atuando de forma antecipada, enquanto a obrigação de compensar (*liability*) está relacionada ao passado e tem como objetivo reparar danos. Eventualmente, pode a *responsibility* também agir de forma retrospectiva, orientando o ofensor sobre como deve proceder após a ocorrência do dano. Por exemplo, quando o autor do ato ilícito procura uma forma de reparação que mais se aproxime de uma restituição *in natura*, já que os danos extrapatrimoniais não são verdadeiramente reparados por compensação financeira (Rosenvald; Braga Netto, 2024).

No âmbito do capitalismo de vigilância, em relação ao tratamento de dados pessoais, a responsabilidade assume duas tendências. A primeira, voltada para os titulares dos dados, envolve a educação digital, ou seja, “capacitação, integrada a outras práticas educacionais, para o uso seguro, consciente e responsável da internet como ferramenta para o exercício da cidadania”, conforme previsto no art. 26 da Lei n.º 12.965/2014 (Marco Civil da Internet). Dessa forma, a educação digital vai além da simples ideia de acesso à internet, abrangendo o conceito de autodeterminação informativa, conforme delineado entre os fundamentos da LGPD. A segunda tendência da responsabilidade é norteada aos agentes de tratamento, implicando a incorporação da ética na realização de suas atribuições (Rosenvald; Braga Netto, 2024).

No campo da área médica, a *responsibility* assume duas vertentes: para os desenvolvedores de dispositivos médicos significa a abertura de espaços para internalização da ética em suas atividades; e para os médicos, a capacitação integrada para a utilização segura, consciente e responsável dos dispositivos médicos que utilizam ferramentas de inteligência artificial.

Em sintonia com o pensamento de Virginia Dignum (2019), *responsibility* refere-se ao papel dos indivíduos em relação aos sistemas de IA. À medida que a cadeia de responsabilidade se expande, são necessários mecanismos para vincular as decisões tomadas pelos sistemas de IA aos seus dados de entrada e às ações das partes interessadas envolvidas no processo de tomada de decisão do sistema. A *responsibility* não se trata apenas de criar regras para governar máquinas inteligentes; ela abrange todo o sistema sociotécnico no qual a

IA opera, incluindo pessoas, máquinas e instituições.

É essencial notar que, independentemente do grau de autonomia, consciência social e habilidade de aprendizado de um sistema autônomo, os sistemas de IA são ferramentas, artefatos criados por pessoas para objetivos específicos. Isso implica que, mesmo que um sistema seja desenvolvido com *responsibility* e transparência, a responsabilidade humana continua insubstituível (Dignum, 2019). Assim, mesmo que o sistema possa se modificar aprendendo com seu contexto de uso, ele o faz com base no propósito determinado pelas pessoas que o programaram. Dessa forma, o fato de que as ações da máquina resultam de aprendizado (*machine ou deep learning*) não isenta seus desenvolvedores de responsabilidade, pois isso é uma consequência dos algoritmos que eles projetaram.

Responsibility refere-se, portanto, ao papel das pessoas no desenvolvimento, fabricação, venda e uso de sistemas de IA. A *responsibility* na IA também é uma questão de regulamentação e legislação, particularmente no que diz respeito à *liability*. Em linhas gerais, a *responsibility* nos sistemas de IA não é apenas uma questão de governança de máquinas inteligentes, mas envolve todo o sistema sociotécnico, incluindo desenvolvedores, usuários e reguladores. Dessa forma, analisada a *responsibility* passa-se a análise da *accountability* no próximo tópico.

2.1.3 *Accountability*

A *accountability* se refere à prestação de contas e transparência em relação às ações e decisões tomadas. Isso implica que os indivíduos ou entidades envolvidas em atividades digitais devem ser capazes de explicar e justificar suas ações, especialmente quando estas têm impacto sobre outros. Na era da informação, isso significa que as organizações devem ser capazes de demonstrar como estão protegendo os dados dos usuários, como estão mitigando riscos de segurança cibernética e como estão cumprindo regulamentações e padrões éticos.

A *accountability* se refere à responsabilidade pelos resultados de ações ou decisões. A *accountability*, ou responsabilização, emerge como um princípio central na governança contemporânea, especialmente no contexto da proteção de dados pessoais e da privacidade. De acordo com Robl Filho (2013), na *accountability* existe a necessidade premente de uma pessoa física ou jurídica que tenha recebido uma atribuição ou delegação de poder, fornecer informações e justificações. Ele ressalta que há uma gama de meios políticos, jurídicos e sociais disponíveis para sancionar essa conduta.

Assim, o termo *accountability* é de suma importância nos domínios da governança,

administração pública, negócios e responsabilidade social. Ele denota a obrigação e responsabilidade de pessoas, organizações ou instituições prestarem contas por suas ações, decisões e pela gestão dos recursos confiados a eles. Em essência, *accountability* representa o princípio essencial de transparência, responsabilidade e prestação de contas (Dignum, 2019).

A *accountability* vertical eleitoral é caracterizado pela avaliação da população através do voto de seus representantes, enquanto o *accountability* vertical social envolve a responsabilização proveniente da imprensa e de organizações da sociedade civil, que expõem publicamente as ações dos agentes estatais, sejam eles eleitos ou não (Robl, 2013).

Por sua vez, a *accountability* horizontal ocorre entre os diferentes poderes, exigindo que os agentes prestem informações e justifiquem suas decisões perante outros agentes estatais. No que diz respeito ao *accountability* judicial, ele se desdobra em três subtipos: o decisional, que diz respeito às informações e justificativas dos magistrados para embasar suas decisões judiciais, o comportamental, que aborda o zelo institucional que os magistrados devem manter, e o institucional, relacionado às ações institucionais que, embora não sejam estritamente judiciais, são componentes essenciais na formação da entidade, incluindo administração, orçamento e relações com os outros poderes (Robl, 2013).

O autor supracitado argumenta que a independência do poder não pode ser usada para criar um poder ilimitado (*unnacountable*), sendo necessário que os outros dois poderes, por meio de mecanismos institucionais, exerçam esse controle (*accountability*). Destarte, a *accountability* busca garantir que os agentes envolvidos em determinada atividade sejam responsabilizados por suas ações e decisões, especialmente em situações em que os danos são causados por sistemas autônomos ou algoritmos.

Em vez de se concentrar apenas na atribuição de culpa após a ocorrência de danos, a *accountability* enfatiza a transparência, responsabilidade e prestação de contas desde a concepção e desenvolvimento dessas tecnologias até sua implementação e uso na prática. Isso significa que todos os envolvidos no ciclo de vida de uma tecnologia, desde os desenvolvedores até os usuários finais, devem ser responsáveis por garantir que ela seja utilizada de forma ética e segura (Chopra; Singh, 2021).

Nesse sentido, a *accountability* pode envolver a implementação de mecanismos de governança, supervisão e controle para garantir a conformidade com os princípios éticos e legais, bem como a prestação de contas por parte dos desenvolvedores e usuários. Além disso, pode incluir a exigência de transparência na tomada de decisões algorítmicas e na operação de sistemas autônomos, permitindo que as partes afetadas entendam como e por que certas decisões foram tomadas.

Moraes (2019) propõe uma estrutura para a adoção de medidas eficazes que demonstrem a conformidade com as regulamentações de proteção de dados pessoais, enfatizando a necessidade de eficácia nessas ações. Segundo a autora, simplesmente evitar violar a lei não é mais adequado; é necessário agir proativamente para prevenir a ocorrência de danos.

No entanto, apesar de seu potencial, a *accountability* enfrenta desafios significativos em sua implementação prática. Isso inclui questões sobre como definir e atribuir responsabilidades em contextos complexos de sistemas autônomos e IA, bem como a necessidade de desenvolver frameworks legais e regulatórios adequados para lidar com essas questões de forma eficaz. Outrossim, conceito de *accountability* não se restringe apenas às organizações privadas, mas também se aplica a entidades governamentais e outras instituições que lidam com dados pessoais.

Em um ambiente cada vez mais digital e interconectado, a proteção da privacidade dos cidadãos é uma preocupação fundamental, e a *accountability* desempenha um papel relevante nesse processo. Desse modo, a questão da responsabilização proativa está relacionada à governança de dados, que pode ocorrer de forma antecipada (*ex ante*) ou após o evento danoso (*ex post*). Dessa forma, alguns aspectos importantes relacionados à *accountability* incluem a transparência, responsabilização social e ética, gestão de recursos e supervisão e fiscalização.

Essa transparência refere-se à prestação de contas que exige a divulgação aberta e honesta das informações pertinentes às ações e decisões tomadas. Isso inclui fornecer informações detalhadas sobre o uso de recursos, políticas, práticas e resultados, bem como identificar quem é responsável pela supervisão das máquinas e como as decisões delas podem ser monitoradas e auditadas. Quanto à responsabilização, ela se relaciona às pessoas ou entidades que são responsáveis por suas ações e devem ser responsabilizadas por quaisquer violações de normas, leis ou regulamentos. Assim, quando as ações ou decisões têm consequências negativas, aqueles que são responsáveis devem enfrentar as consequências e tomar medidas corretivas, se necessário.

Nesse tipo de *accountability*, também está implícita a responsabilidade social e ética de agir de maneira que beneficie a sociedade e minimize impactos negativos. Isso pode incluir a consideração dos interesses das partes interessadas, além do cumprimento de regulamentos e padrões éticos. Além disso, a *accountability* em organizações está relacionada à gestão eficiente dos recursos, garantindo que os recursos financeiros, humanos e outros sejam usados de maneira apropriada e responsável. Em muitos casos, a *accountability* é reforçada por

órgãos de supervisão, reguladores ou sistemas de verificação independentes que monitoram e avaliam as atividades das partes responsáveis.

2.1.4 *Answerability* - Explicabilidade

Na sequência, é importante refletir sobre a *answerability*, que pode ser traduzida como "explicabilidade", ou seja, capacidade de explicação. Essa acrescenta outra dimensão à natureza preventiva da responsabilidade, demonstrada pelo dever mútuo de promover a confiança através da transparência.

Segundo inferem os doutrinadores Rosenvald e Braga Netto (2024) a *answerability* é um processo de justificação mútua das decisões que vai além do simples direito à informação, permitindo a compreensão completa do contexto da operação. Ora, a *answerability* refere-se à capacidade de responder por nossas ações e decisões perante as partes afetadas. Isso implica não apenas assumir a responsabilidade pelas consequências de nossas ações, mas também estar disposto a prestar contas e enfrentar as consequências, se necessário. Logo, nas novas descobertas científicas, isso pode se traduzir em empresas sendo responsáveis por violações de dados ou práticas antiéticas, e estarem sujeitas a ações corretivas ou punitivas por parte das autoridades reguladoras ou da opinião pública.

Novas pesquisas têm sido feitas sob a denominação de *Explainable Artificial Intelligence* (XAI). Neste ponto, importante destacar a diferença entre *explainability* e *explicability*. *Explainability* tende a se concentrar mais na capacidade técnica de um sistema de explicar suas decisões de uma forma que os humanos possam entender, frequentemente de forma associada à área de design e operação de sistemas de IA, sendo, portanto, um requisito operacional do sistema de IA. *Explicability*, por outro lado, pode abranger aspectos mais amplos, como a necessidade ética e regulatória de proporcionar transparência. Dessa forma, a *explicability* implica uma exigência normativa, incorporando considerações sobre por que e como as explicações devem ser fornecidas, focando na justiça, equidade e *accountability* (Shademan *et al*., 2016).

Nesse sentido, a *explainability* acrescenta outra dimensão à natureza preventiva da responsabilidade, demonstrada pelo dever mútuo de promover a confiança através da transparência que é princípio taxativamente previsto no art. 6º, VI da LGPD[4]. A confusão entre interpretabilidade e explicabilidade, denominada 'confusão interpretabilidade-

[4] "Art. 6º […] VI – transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial".

explicabilidade', é bastante disseminada. Estudos recentes mostram que há uma tendência de equiparar modelos interpretáveis a modelos explicáveis, mesmo entre cientistas de dados altamente qualificados. A distinção entre essas funções é importante, especialmente quando as saídas algorítmicas precisam ser plausíveis para que os usuários possam desafiá-las em situações críticas, como na saúde e condução autônoma (Herzog, 2022).

Ao passo que a *liability*, *responsibility* e *accountability* focalizam no indivíduo que realiza uma ação ou comporta-se de maneira prejudicial ou potencialmente prejudicial - denominados agentes de responsabilidade, a *answerability* (ou *explainability*) - se concentra na outra extremidade dessa dinâmica: os destinatários ou sujeitos da responsabilidade, que têm o direito de demandar explicações sobre ações e decisões tomadas pelo indivíduo no controle da atividade ((Rosenvald; Faleiros Júnior, 2023).

Em outras palavras, a *answerability* enfatiza a importância de não apenas identificar as causas e os agentes por trás de ações e decisões, mas também de garantir que esses agentes possam ser questionados e tenham que prestar contas. Adotando uma perspectiva relacional, a responsabilidade entendida como *answerability* fornece uma razão adicional para proteger o ser humano, mostrando-se extremamente valiosa em contextos de adoção generalizada de sistemas de inteligência artificial.

Portanto, a questão central não é apenas identificar a IA em uso e suas funcionalidades, mas enfrentar um desafio de natureza ontológica: é essencial entender como se aplicam os princípios de prevenção e precaução da responsabilidade civil, para que se possa medir as expectativas sobre cada envolvido na atividade, especialmente em relação à capacidade de antever possíveis efeitos.

Neste aspecto, importante ressaltar a diferença dos princípios da prevenção e da precaução para uma melhor análise do gerenciamento de riscos. O princípio da precaução é empregado em situações onde não há certeza científica completa sobre os riscos potenciais de uma atividade. Esse princípio orienta a adoção de medidas preventivas mesmo na ausência de evidências concretas de dano. O foco está na prevenção de riscos que ainda não são completamente entendidos ou quantificados, lidando com o risco incerto. Esse princípio é proativo em mitigar o perigo abstrato, o que significa que age antes que qualquer dano potencial se torne uma realidade conhecida. Assim, ele se baseia mais na prudência e na gestão da incerteza, sem necessariamente esperar pela comprovação do dano para agir (Wedy, 2015).

Por outro lado, o princípio da prevenção é aplicado quando os riscos de uma atividade são conhecidos e bem documentados cientificamente. Este princípio se concentra em evitar

danos que são cientificamente previstos ou já evidenciados, tratando do risco certo, conforme delineado por Milaré (2015). A prevenção envolve medidas para barrar o perigo concreto, isto é, para intervir antes que um dano conhecido e comprovadamente possível ocorra. Este princípio tem uma abordagem mais direta e é menos especulativo em relação ao tipo de intervenções que são necessárias (Santos, 2020).

Em síntese, percebe-se que a prevenção cuida de riscos certos ou perigos concretos, já conhecidos pelo meio científico. De outro lado, a precaução busca gerir riscos desconhecidos, incertos ou perigos abstratos.

Em regimes democráticos, sempre se considerou justo que quem realiza uma ação tenha condições de explicar aos afetados o motivo de suas ações, decisões ou recomendações. Exigir explicações é um direito legítimo, uma vez que decisões e ações precisam ser compreensíveis para serem consideradas responsáveis. No contexto da Lei Geral de Proteção de Dados (LGPD), o conceito de *answerability* se expande para incluir a capacidade de contestação, significando que o titular dos dados tem o direito de solicitar a revisão de decisões feitas exclusivamente por meio de processamento automatizado de dados pessoais que impactem seus interesses. Isso inclui decisões que afetam a definição de perfis pessoais, profissionais, de consumo e crédito, ou traços da personalidade, conforme estabelecido no artigo 20 da Lei nº 13.709/18 - LGPD. A pessoa tem o direito de se opor à criação de perfis (*profiling*), solicitar sua exclusão ou correção, ou contestar decisões automáticas relacionadas a si.

Dessa maneira, estamos diante do conceito conhecido como direito à explicação "*right to an explanation*", presente no GDPR (*General Data Protection Regulation*), que se refere à obrigação de esclarecer decisões automatizadas específicas de maneira compreensível para os indivíduos afetados. Isso não implica necessariamente em revelar todos os detalhes técnicos ou o funcionamento interno da "*black-box*" utilizada para tomar a decisão. Em vez disso, basta fornecer uma explicação que ainda não aconteceu, permitindo ao indivíduo entender o que precisaria ser alterado para obter um resultado diferente (Rosenvald; Faleiros Júnior, 2023).

A *answerability* refere-se à capacidade de responder por nossas ações e decisões perante as partes afetadas. Isso implica não apenas assumir a responsabilidade pelas consequências de nossas ações, mas também estar disposto a prestar contas e enfrentar as consequências, se necessário. Portanto, engloba não apenas a ideia de que respostas existem, mas também a capacidade de responsabilizar indivíduos ou organizações pelos resultados de suas ações ou das ferramentas que utilizam. Para assegurar a atuação ética de sistemas

inteligentes, não basta tentar incorporar princípios éticos diretamente nos sistemas, como muitas vezes é proposto. É necessário, em vez disso, projetar esses sistemas para funcionarem de maneira efetiva dentro de contextos específicos, incluindo ambientes que permitam supervisão e avaliação (Rosenvald; Faleiros Júnior, 2023).

Dessa forma, a dinâmica da explicabilidade envolve a identificação dos agentes responsáveis e da natureza da responsabilidade. De tal modo, a explicabilidade se preocupa em saber: a quem ela se destina? Quais resultados são contemplados e com que finalidade? Nesse sentido, Frank Pasquale (2017) introduziu a "quarta lei da robótica", que exige que os robôs indiquem a identidade de seus criadores, controladores ou proprietários.

Entender quem deve prestar contas, os motivos por trás disso e os destinatários dessas explicações nos aproxima do princípio de supervisão ou *oversight*. Esse conceito representa um elemento de governança em que uma entidade com autoridade especial tem a capacidade de examinar provas de ações e vinculá-las a suas consequências (Rosenvald; Faleiros Júnior, 2023).

Como discutido por Herzog (2022), a explicabilidade vai além da mera interpretabilidade mecânica, exigindo interfaces adaptadas ao destinatário e ao caso de uso. Essas interfaces devem incorporar uma variedade de formas de explicações que podem não ser completas, mas que permitem aos *stakeholders* (partes interessadas) assumir responsabilidade. A flexibilidade da explicabilidade permite que ela não exija explicações mecanicistas em todos os níveis de uso, mas sim o nível necessário para servir princípios éticos como beneficência, não maleficência e autonomia.

A supervisão funciona como um complemento aos mecanismos regulatórios de governança, como a *accountability*, possibilitando a implementação de verificações e balanços em processos onde comportamentos ideais não possam ser previamente definidos de forma regrada. Em uma abordagem *ex post*, a entidade supervisora pode distinguir entre comportamentos aceitáveis e inaceitáveis, mesmo quando comportamentos específicos não possam ser antecipadamente definidos. Adicionalmente, mesmo na presença de regras, a supervisão pode assegurar que as ações foram executadas de maneira consistente, levando em conta as especificidades de cada situação.

A *answerability* não exige a exposição detalhada da essência causal que leva a uma decisão ou ação. Assim, não implica necessariamente na divulgação completa de todos os processos causais que levam a uma decisão. Em vez disso, foca-se em possibilitar a identificação de aspectos relevantes que podem ser questionados e avaliados. Isso significa priorizar uma abordagem que permita revisões extrajudiciais por humanos de decisões

algorítmicas, promovendo um equilíbrio entre a eficácia tecnológica e a *accountability* social.

Rosenvald e Faleiros Júnior abordam a concepção de *answerability* como uma expansão do conceito de responsabilidade na esfera da tecnologia, especialmente em relação aos algoritmos e à IA. O termo *answerability* é traduzido como "explicabilidade" e se relaciona intimamente com a transparência algorítmica, convergindo para a ideia de que os desenvolvedores e operadores de sistemas algorítmicos devem fornecer justificações compreensíveis para suas ações, particularmente quando estas têm o potencial de afetar significativamente indivíduos ou a sociedade (Rosenvald; Faleiros Júnior, 2023).

Os autores defendem que além de serem informados sobre os processos decisórios automáticos que os afetam, os indivíduos têm o direito de exigir explicações sobre essas decisões, alinhando-se assim com conceitos de governança responsável e ética em tecnologia. Isso também se alinha com princípios estabelecidos em regulamentos globais como o GDPR, que exige a explicabilidade das decisões automatizadas (Rosenvald; Faleiros Júnior, 2023).

Ressaltam, ainda, Rosenvald e Faleiros Júnior (2023) a importância da prevenção e da precaução no desenvolvimento de algoritmos, propondo que os operadores de IA atuem como "fiduciários de informação", garantindo não só a segurança, mas também a justiça e equidade dos sistemas que criam. Além disso, enfatiza a importância de um componente de supervisão que permita a verificação e o controle das atividades algorítmicas, garantindo que as regras sejam aplicadas consistentemente e que os comportamentos sejam analisados dentro de contextos específicos.

Em suma, a *answerability* ressalta a importância de criar sistemas de IA que operem de maneira transparente e responsável a fim de fortalecer a obrigação das consequências imprevisíveis, focando na necessidade de atribuir e explicar a autoria e controle dos sistemas robóticos.

3 NEXO CAUSAL NA ERA DA INOVAÇÃO: ANÁLISE JURÍDICA DA CIRURGIA ROBÓTICA E A TEORIA DO RISCO DO DESENVOLVIMENTO

Na era da inovação tecnológica, a introdução de inteligências não naturais e robótica na medicina, especialmente nas cirurgias, traz à tona desafios complexos relacionados ao nexo causal e à compensação dos danos. A crescente autonomia dos sistemas inteligentes em

procedimentos cirúrgicos exige uma reavaliação dos conceitos tradicionais de responsabilidade, pois esses sistemas podem falhar ou apresentar comportamentos inesperados. Nesse contexto, a teoria do risco do desenvolvimento emerge como uma abordagem relevante para entender as implicações jurídicas dessas tecnologias avançadas. A análise jurídica da cirurgia robótica à luz dessa teoria busca esclarecer como o desenvolvimento tecnológico pode impactar o nexo causal, destacando a necessidade de um marco regulatório que contemple tanto a inovação quanto a segurança e a *accountability*, garantindo a proteção dos direitos e interesses de todas as partes envolvidas.

3.1 CONSIDERAÇÕES INICIAIS SOBRE O NEXO CAUSAL

A negligência nos estudos sobre o nexo causal pode ser atribuída à forte influência moral que, historicamente, destacava a culpa como elemento central da responsabilidade civil. Quando a culpa era comprovada, a relação de causalidade era automaticamente presumida como certa. Contudo, nas práticas contemporâneas, a responsabilidade objetiva, que não exige a comprovação de culpa, destaca a importância da determinação do nexo causal como meio de isentar a obrigação de indenizar por parte do causador do dano (Rosenvald; Braga Netto, 2024).

Essa mudança implica na adoção de um raciocínio mais objetivo e técnico por parte dos juízes, elevando a autonomia e valorizando o pressuposto do nexo causal. Este último torna-se a chave para identificar a responsabilidade, o responsável e os danos pelos quais deve ser responsabilizado (Rosenvald; Braga Netto, 2024).

O nexo causal, referindo-se à conexão entre a ação ou evento (conduta do agente) e o resultado (dano), desempenha um papel relevante no contexto da responsabilidade civil. Para que alguém seja responsável por um dano, é essencial estabelecer um vínculo causal claro entre a ação e o resultado prejudicial, ou seja, a ação deve ser a causa direta do dano (Viola, 2023).

O dano, portanto, se conecta, em uma relação causal, a ação ou omissão. Inexistindo o nexo de causalidade não há responsabilidade civil, uma vez que ausente a conexão entre o dano e a conduta/atividade do agente. Assim, para haver responsabilização civil, antes de mais nada, deve estar presente e comprovado o nexo causal decorrente do evento danoso e ação ou omissão do ofensor, bem como ausente qualquer das excludentes do nexo causal, como exemplo culpa exclusiva da vítima ou de terceiro, caso fortuito ou força maior.

Para compreender o nexo causal, a doutrina tradicional fala em vínculo fático, não

jurídico, sendo a ligação ou relação de causa e efeito entre a conduta e o resultado. Nesse sentido, o princípio da prevenção determina que, quando o nexo entre a causa e o dano é conhecido, deve-se sempre que possível evitar o dano, removendo a sua causa. Portanto, a certeza do dano e a consciência da conexão causal entre o agente causador e o dano são elementos indispensáveis para a implementação do princípio da prevenção (Santos, 2020).

Por outro lado, a concepção contemporânea entende que a causalidade é um juízo de imputação jurídica (Braga Netto, 2024). O nexo não é mais apenas naturalístico, ele é sobretudo imputacional. Se refere à investigação não só de quem causou o dano, mas quem vai responder por ele. Nesse sentido, pode se dizer que uma empresa poderá responder civilmente, mesmo que não tenha dado causa a um dano, se este pertencer a sua esfera de risco (Braga Netto, 2024).

O nexo causal desdobra-se em duas vertentes essenciais: a causalidade naturalística e a causalidade jurídica. Ambas são fundamentais para determinar os direitos e deveres das partes envolvidas em um caso. Hume (1988), filósofo iluminista escocês, contribuiu significativamente à discussão sobre causalidade, argumentando que ela é inferida da repetição de eventos, questionando a certeza da relação de causa e efeito. Sua inovação filosófica esclareceu que a "necessariedade" não é uma ligação misteriosa, mas derivada da experiência humana.

Seguindo Hume, John Stuart Mill desenvolveu a ideia de causalidade como uma relação constante e invariável entre eventos, trazendo contribuições importantes sobre "complexidade e pluralidade" (Viola, 2023, p. 87). Contribuições adicionais de Hart e Honoré distinguiram entre causalidade necessária e causalidade suficiente (Hart; Honoré, 1985).

A análise do nexo causal é realizada por uma variedade de doutrinadores em duas etapas, apurando a cadeia causal naturalística e investigando a causa legal. Essa análise divide-se em causalidade naturalística e jurídica. A causalidade naturalística refere-se à relação direta entre a ação e suas consequências, desempenhando um papel importante na identificação das origens de um dano. Já a causalidade jurídica avalia a responsabilidade legal das partes envolvidas, indo além da relação de causa e efeito para determinar a imputação legal ao responsável (Rosenvald; Braga Netto, 2024).

O princípio da causalidade emerge como ideia central na teoria da responsabilidade civil, determinando quem deve assumir as consequências dos riscos gerados (Viola, 2022). A análise do nexo causal, embora incontroversa entre os autores, enfrenta a dificuldade prática de definir precisamente a causa no caso concreto. Essa análise examina cuidadosamente os fatos conhecidos ou determináveis, buscando determinar se o evento foi uma condição

contribuinte para o resultado, considerando a perspectiva de uma pessoa razoável (Pires, 2019).

A causalidade trata do entendimento do que realmente ocorreu em um caso específico, ou seja, identificar o que causou determinado evento. Essa interpretação factual é geralmente considerada algo evidente e facilmente resolvido pelo bom senso entre os especialistas jurídicos. Em contrapartida, a causalidade legal é vista como problemática e, portanto, interessante. Ela envolve um conjunto de critérios a serem aplicados quando não há uma interpretação factual clara e de bom senso do caso, ou quando, mesmo havendo uma interpretação causal clara, considerações de políticas jurídicas (como a previsibilidade) devem ser aplicadas, resultando em uma interpretação causal diferente. Exemplos típicos onde se deve usar uma interpretação causal legal, devido à ausência de uma interpretação factual clara, são os chamados casos de sobredeterminação (Lehmann; *et al*., 2004).

A quebra do dever jurídico deve ser a causa da violação do bem jurídico. Nesse contexto, a doutrina alemã faz uma distinção entre "a causalidade que fundamenta a responsabilidade (haftungsbegründende Kausalität) e a causalidade que completa a responsabilidade (haftungsausfüllende Kausalität)" (PIRES, 2019, p. 104). Resumidamente, é necessária uma dupla comprovação da causalidade: deve haver um vínculo causal entre a conduta ilícita e a violação do bem jurídico, bem como esta última e o dano.

A necessidade de diferenciar as funções do nexo causal na responsabilidade civil evidencia o erro cometido por parte da doutrina ao examinar o nexo de causalidade com base em teorias aceitas acriticamente (Gama; Viola, 2021).

Apesar da concordância quanto à necessidade do nexo causal, a verdadeira dificuldade prática reside na definição precisa da causa no contexto do caso específico. A abordagem sob a perspectiva da causalidade visa delimitar a responsabilidade pelo dano. O desafio prático está em definir de forma precisa a identidade da causa no caso concreto, considerando os eventos extraordinários e inéditos enfrentados pela humanidade, ou seja, se a vantagem foi verdadeiramente resultado do ato ilícito, estabelecendo assim a conexão entre os benefícios obtidos pela vítima e o evento danoso que deu origem à indenização (Sanseverino, 2010).

Muitas abordagens doutrinárias teóricas foram desenvolvidas para explicar a relação causal, merecendo destaque histórico a teoria da equivalência das condições, a teoria da causalidade adequada e a teoria da causa direta e imediata.

A teoria da equivalência das condições, também nominada teoria *sine qua non*, foi desenvolvida por Von Buri em 1860 e, posteriormente, aperfeiçoada por outros estudiosos, tornou-se um marco para os estudos do nexo causal. Tal teoria diz que todas as condições se

representam, ou seja, não é necessário determinar a maior ou menor proximidade entre a conduta do agente e seus efeitos, pois qualquer condição se transforma em uma causa, independentemente da sua correlação com o dano ser mais ou menos direta. Doutrinadores franceses, ao aprimorar a teoria da *"equivalence des conditions"*, entenderam que o dano é resultado de um conjunto de fatos decorrentes de uma ação ou omissão humana, além de circunstâncias externas (Rosenvald; Braga Netto, 2024, p. 953). Dessa forma, a teoria reconhece que mesmo causas remotas podem ser consideradas relevantes para o estabelecimento do nexo causal, enfatizando a importância das condições antecedentes na determinação da responsabilidade por um dano.

Pela teoria da causalidade adequada podemos perceber um aprimoramento científico ao incorporar uma análise jurídica da causalidade, em contraste com a abordagem meramente naturalista proposta pela teoria da equivalência dos antecedentes causais. A teoria da causalidade adequada utiliza presunções fundamentadas na probabilidade e previsibilidade dos eventos. Dessa forma, uma condição é considerada causa somente quando, após análise do caso, o magistrado identifica que o dano condiz, de maneira abstrata, ao caminho natural dos acontecimentos. Em outras palavras, o dano sofrido pela vítima é um efeito usualmente previsível do fato, segundo entendimento da experiência comum. Portanto, essa teoria assenta-se na probabilidade de ocorrência do evento danoso (Rosenvald; Braga Netto, 2024).

Apesar das intensas discussões teóricas sobre o tema, desde a implementação do Código Civil de 1916, tanto na doutrina quanto na jurisprudência, afirma-se que o dever de reparar só pode ser atribuído ao agente cujo ato foi a causa direta e imediata do prejuízo. Portanto, o acolhimento da teoria da causa direta e imediata, também denominada teoria da interrupção do nexo causal refere-se à previsão do inadimplemento das obrigações negociais, disposta no art. 403 do CC/2022, assim como à responsabilidade extracontratual (Tepedino, 2019).

No âmbito doutrinário, foi incorporada à teoria da causa direta e imediata a noção, frequentemente chamada de subteoria da necessidade da causa. Essa perspectiva estabelece que a obrigação de indenizar emerge quando o dano é um resultado inevitável de uma causa específica. A irrelevância da causa, portanto, não se dá pela sua distância em relação ao dano, mas sim pelo surgimento de uma causa alternativa capaz de gerar o mesmo efeito. As maiores complicações aparecem quando múltiplas causas concorrem para o mesmo resultado lesivo, e cabe ao juiz determinar a qual delas atribuir a responsabilidade pela reparação. Eliminando-se a análise da imprevisibilidade do dano passível de indenização, estas situações podem ser examinadas à luz dos princípios gerais sobre a interrupção do nexo de causalidade (Tepedino;

Silva, 2019).

3.2 NEXO CAUSAL E IA AUTÔNOMA

A causalidade no contexto da inteligência artificial autônoma apresenta desafios significativos, uma vez que as decisões desses sistemas são influenciadas por vastos conjuntos de dados e algoritmos complexos. Identificar uma única causa direta para um resultado específico torna-se difícil, pois a causalidade pode estar distribuída por elementos como a programação inicial, o conjunto de dados de treinamento e as interações em tempo real.

Se o algoritmo suspeito de causar o dano for desenvolvido ou alterado por um sistema de IA usando técnicas de *machine learning* e *deep learning*, a relação causal entre a lesão e o comportamento do sujeito torna-se desafiadora, caracterizando a chamada "causalidade complexa" (Barbosa, 2021, p. 166).

Em sistemas de inteligência artificial autônoma, a cadeia de eventos que leva a um resultado específico frequentemente é complexa e difícil de rastrear. A atribuição convencional de culpa complica-se quando há múltiplos agentes envolvidos, como os criadores do algoritmo, desenvolvedores de software e o próprio sistema autônomo. Diante disso, parte da doutrina considera que a responsabilidade civil é inadequada para enfrentar os desafios das novas tecnologias, especialmente as que empregam aprendizado profundo, pois as estruturas clássicas baseadas na culpa não conseguem distinguir claramente entre danos causados por erro humano e aqueles provenientes do próprio algoritmo (Barbosa, 2021).

A complexidade aumenta com atualizações do software fornecidas por um sujeito diferente do produtor original. Determinar se o mau funcionamento do algoritmo decorre da programação inicial ou de modificações nas atualizações torna-se difícil. Essa incerteza pode suscitar questões relacionadas à causalidade alternativa, especialmente quando múltiplas causas, muitas desconhecidas, convergem.

Algoritmos de IA autônoma podem aprender e evoluir de maneiras imprevisíveis, dificultando a previsão de seu comportamento futuro e tornando desafiador antecipar os riscos associados. Desse modo, a autonomia de um robô, que tem a capacidade de aprender e se adaptar independentemente, pode resultar em ações imprevisíveis. Esses comportamentos podem levar a danos que não derivam diretamente de sua programação original. Segundo Matthias (2004), as normas convencionais de responsabilidade legal não seriam suficientes para lidar com essas máquinas imprevisíveis, dado que os seres humanos perderiam o controle efetivo sobre as ações do robô.

Uma visão semelhante é expressa na Resolução do Parlamento Europeu de 16 de fevereiro de 2017, relativa às regras de direito civil aplicáveis à robótica. Essa resolução argumenta que o marco legal existente é inadequado para abordar os danos causados por robôs que possuem habilidades de adaptação, aprendizado e autonomia, uma vez que essas características introduzem um elemento de imprevisibilidade em seus comportamentos.

No entanto, esta perspectiva não é totalmente persuasiva por várias razões. Inicialmente, para que o comportamento de um robô seja classificado como imprevisível, é necessário que ocorra uma descontinuidade significativa em relação à sua programação original. Isso indica que meras anormalidades, como falhas de sensores, erros de programação, bugs de software ou defeitos de hardware, ainda são consideradas previsíveis (por exemplo, um robô assistente pessoal que administra uma dose de medicamento 100 vezes maior do que o indicado ainda agiria de forma previsível se tal ação estivesse alinhada com suas funções programadas, ao contrário dele se declarar poeta em vez de médico, o que seria verdadeiramente imprevisível). Atualmente, é raro encontrar exemplos de comportamentos verdadeiramente imprevisíveis em robôs nesse sentido. Isso acontece porque, mesmo quando um robô aprende algo novo de forma independente, ele o faz dentro dos limites estabelecidos pelos programadores iniciais, que definem seus objetivos (O´Sullivan; *et al*, 2019).

Da mesma forma, cada robô é projetado fisicamente para tarefas específicas, e mesmo aprendendo novas e imprevisíveis habilidades, sua estrutura física limita a execução de ações que não sejam compatíveis com sua configuração material (O´Sullivan; *et al*, 2019). Se o comportamento de um robô se tornar imprevisível a ponto de causar danos, isso indica que o dispositivo não oferece segurança adequada para os humanos, podendo levar a exigências legais para sua remoção do mercado. Além disso, tal imprevisibilidade pode ser vista como evidência de um defeito inerentemente perigoso no robô, situação que poderia ser objeto de responsabilidade civil por defeito do produto.

A presença de múltiplas causas e a dificuldade em isolar a contribuição de cada uma introduzem incertezas sobre a causalidade. Em danos causados por IA, pode ser desafiador determinar se o dano resultou de uma ação autônoma específica ou de outros fatores. A doutrina denomina isso como causalidade alternativa incerta, pois as causas subjacentes dos comportamentos de IA frequentemente são desconhecidas, tornando difícil estabelecer uma conexão clara entre a ação da IA e o dano causado (Barbosa, 2021).

Ao avaliar a causalidade, a ponderação judicativa deve manter-se alinhada com a proposta apresentada em relação ao requisito, compreendido à luz de um sentido imputacional (Barbosa, 2021, p. 167). Os modelos tradicionais de responsabilidade civil, muitas vezes

baseados em noções simplificadas de causa e efeito, enfrentam limitações ao lidar com a complexidade e dinâmica das inteligências artificiais autônomas.

Mateus de Oliveira Fornasier destaca a importância de sopesar cuidadosamente o nexo de causalidade entre o uso da máquina e o dano perpetrado (Fornasier, 2022). Portanto, a análise do liame causal torna-se essencial nesse contexto.

A transparência no entendimento dos modelos de inteligência artificial é essencial para avaliar a responsabilidade civil em situações onde danos possam surgir. Cerka destaca a probabilidade de falhas em software altamente complexo, especialmente quando desenvolvido por várias mãos. A dificuldade em atribuir responsabilidade a falhas que surgem em camadas diversas do desenvolvimento de software torna-se ainda mais desafiadora à medida que robôs e programas artificialmente inteligentes aprendem a modificar seu próprio código (Cerka *et al*., 2015).

O sistema jurídico, é sabido,

> *"no solo crea normas, sino que también introduce valores, algunos de elos constantes y outros mutantes, proprio de los procesos sociales y que geran crisis, ingobernabilidad en determinadas oportunidades, que se materializan en daños y que las personas buscan constantemente la reparación de los mismos"* (Ghersi; Weingarten, 2008, p. 17).

Considerando o comportamento inesperado dos robôs de inteligência artificial (IA) em relação aos humanos que os desenvolveram ou operam, surge a questão sobre se a capacidade de realizar ações imprevistas pelas máquinas inteligentes poderia quebrar a conexão causal entre as ações do programador, do operador ou do usuário e os danos resultantes. Torna-se difícil estabelecer uma ligação causal direta entre uma lesão e as ações de um indivíduo. Existe uma lacuna evidente entre o momento da criação e programação da IA e seu desenvolvimento autônomo subsequente, impulsionado pelo aprendizado profundo (*deep learning*), de forma que o criador não pode prever completamente — ao menos não de forma absoluta — os comportamentos futuros das máquinas (Mello, 2022).

As decisões judiciais têm adaptado e expandido os conceitos de culpa, dano, nexo causal e outros elementos essenciais da responsabilidade civil, incluindo teorias como risco criado, risco proveito, risco integral e risco do desenvolvimento. Independentemente da interpretação do nexo causal, todas as teorias da causalidade destacam que o evento considerado como causa não pode ser removido da situação sem que o resultado desapareça. Busca-se, assim, uma análise cuidadosa dos fatos conhecidos ou determináveis do caso concreto para precisar se o evento foi uma condição para o resultado danoso (Pires, 2019).

Por outro lado, Hironaka e Mulholland (2010) sustentam a tese de que no sistema

jurídico brasileiro, o conceito de nexo causal está passando por um processo de flexibilização, e existe uma crescente necessidade de implementar uma ferramenta que presuma a causalidade em certos contextos específicos. Assim, Mulholland defende a utilização de três requisitos para se presumir o nexo causal, quais sejam: que a descrição do evento danoso seja feita de maneira precisa, identificando claramente o dano e a conduta a ele associada; descrever adequadamente a decomposição da cadeia causal, indicando a causa ou as causas essenciais (*sine qua non*) do dano e utilizar técnicas estatísticas por meio de análises periciais, que possam calcular cientificamente a probabilidade de uma determinada atividade ou conduta ter sido a causadora do dano (Mulholland, 2010).

À medida que avançamos na compreensão da aplicação de conceitos tradicionais de responsabilidade civil ao contexto da IA autônoma, observa-se uma necessária evolução nas abordagens jurídicas. A autonomia crescente dos sistemas de IA coloca desafios únicos sobre o tradicional entendimento de nexo causal, uma vez que as ações desses sistemas podem ser indeterminadas ou emergir de processos de aprendizado contínuo que não foram explicitamente programados por humanos.

Diante desse panorama, a flexibilização do nexo causal, como sugerida por Hironaka e Mulholland, pode ser particularmente pertinente. A presunção de causalidade, apoiada por descrições precisas e análises técnicas, oferece um meio viável de lidar com a complexidade inerente às interações mediadas por IA. Isso não só facilita a atribuição de responsabilidade, mas também promove um equilíbrio entre a inovação tecnológica e a proteção aos direitos dos indivíduos afetados. Dessa feita, analisado o nexo causal e a IA autônoma, passa-se no próximo tópico a análise do nexo causal especificamente na área da saúde.

3.3 DO NEXO CAUSAL NA ÁREA DA SAÚDE

A revolução tecnológica na área da saúde trouxe avanços significativos, possibilitando que médicos realizem procedimentos cirúrgicos em pacientes localizados em regiões remotas do mundo. A inteligência artificial e a robótica têm desempenhado um papel expressivo nesse cenário, proporcionando o desenvolvimento de robôs de assistência inteligentes para cuidados médicos, especialmente, na cirurgia minimamente invasiva, como nas áreas de urologia, ginecologia, cirurgia geral, toráxica, abdominal e neurocirurgia, o uso de robôs tem se destacado, proporcionando maior precisão e segurança ao procedimento.

No entanto, a complexidade na análise da responsabilidade civil na cirurgia robótica reside na determinação da gênese do dano e na atribuição do dever de indenizar. A utilização

de dispositivos cirúrgicos assistidos por robôs – *Reference Architecture for Space Data Systems* (RASDs) introduz um novo conjunto de desafios legais quando falhas ocorrem durante procedimentos médicos. A responsabilidade por danos decorrentes de erros nesse contexto levanta questionamentos sobre quem deve ser responsabilizado: o médico que opera o RASD ou o fabricante do dispositivo (Nogaroli, 2023).

Aqui cabe fazer uma definição de erro médico a fim de se perquirir quem deve reparar o dano. Erro médico é frequentemente caracterizado como um ato não intencional, seja por omissão ou comissão, que não alcança seu resultado desejado. Isso inclui falhas na execução de uma ação planejada (erros de execução), a adoção de um plano inadequado para atingir um objetivo (erros de planejamento) ou desvios no processo de cuidado que podem ou não causar danos ao paciente. Os danos aos pacientes decorrentes de erros médicos podem ocorrer tanto em nível individual quanto sistêmico (Makary; Daniel, 2016).

Na visão de Nogaroli (2023), a complexidade na análise da responsabilidade civil na cirurgia robótica exige a determinação da causa eficiente do dano, considerando se decorreu de serviço essencialmente médico, paramédico ou extramédico. Para atribuir a responsabilidade por eventos adversos, é necessário analisar se o dano resultou de atos praticados exclusivamente pelos profissionais da medicina, envolvendo formação e conhecimentos médicos. Caso a culpa seja do médico, o hospital pode responder solidariamente. No caso de serviço paramédico, a responsabilidade objetiva do hospital pode incidir pelos atos da equipe de enfermagem. Já no serviço extramédico, relacionado à instalação inadequada do aparato robótico, a responsabilidade objetiva do hospital também é considerada.

Assim, ao adentrar a análise detalhada dessa problemática no ordenamento jurídico brasileiro, é essencial seguir uma metodologia que leve em conta a origem do dano e a natureza do serviço prestado na cirurgia robótica. Ao analisar a teoria de responsabilidade civil no âmbito da automação substitutiva e complementar, torna-se crucial distinguir entre situações em que a inteligência artificial substitui completamente a atuação humana e aquelas em que ela apenas complementa as habilidades profissionais (Pasquale, 2020).

Para promover maior responsabilização dos fornecedores de IA e, ao mesmo tempo, apoiar a experiência dos médicos, a responsabilidade estrita é sugerida quando a IA substitui integralmente os profissionais médicos. A aplicação de padrões de responsabilidade estrita (*liability*) implica que, em caso de eventos adversos, o fabricante, distribuidor e varejista do produto podem ser responsabilizados, mesmo na ausência de negligência. Esse padrão favorece melhorias contínuas na tecnologia e evita padrões elevados que poderiam

desestimular a inovação. Nos casos em que a IA complementa as habilidades dos profissionais, a responsabilidade ainda deve ser atribuída, mas de maneira diferente (Pasquale, 2020).

A interpretação expansiva da doutrina do intermediário erudito, que exige que o fabricante forneça avisos adequados sobre o potencial de danos da tecnologia, pode ser desafiadora quando a robótica complementar não cumpre suas promessas. Nesses casos, a responsabilidade não deve recair exclusivamente sobre o médico, e padrões mais rigorosos para máquinas que prometem substituir os profissionais são defendidos. A distinção entre automação substitutiva e complementar é crucial para evitar a automação prematura em setores onde a experiência humana é essencial (Pasquale, 2020).

Na área médica, onde a supervisão competente é tradicionalmente necessária, a responsabilidade estrita pode garantir compensação em caso de eventos adversos evitáveis. Em termos de incentivo à melhoria na IA e prática médica, padrões de responsabilidade adequados são essenciais (Pasquale, 2020). Nesse sentido, Sheriff (2015) sugere uma adaptação da proposta de *digital peculium* (pecúlio digital) de Ugo Pagallo para lidar com "casos difíceis" em que robôs completamente autônomos realizam escolhas sem uma conexão clara com o programador original, escapando, portanto, das previsões de incerteza inicialmente programadas. Ao contextualizar esses "casos difíceis" dentro das amplas perspectivas da teoria ética e jurídica, como descrito por H.L.A.

Hart e Ronald Dworkin, Sheriff (2015) questionam se é possível determinar uma resposta definitiva, ou se permanece uma indefinição, sobre a responsabilidade legal diante da autonomia avançada dos robôs. Considerando que a autonomia total ainda não é uma realidade na cirurgia robótica, o foco recai sobre a aderência às normativas legais vigentes e sobre o debate a respeito da necessidade de futuras modificações nessas regras.

Menos exigências podem levar à diminuição da experiência distribuída, fundamental para o avanço médico. Nos Estados Unidos, esse desafio resultou em casos conhecidos como *"finger-pointing"*, nos quais surge a importante questão de quem deve ser responsabilizado por danos ocorridos durante procedimentos cirúrgicos robóticos: o médico (e/ou o hospital) ou o fabricante do equipamento (Nogaroli, 2023).

Nesse sentido, um dispositivo com nome de *dVLogger* foi desenvolvido em semelhança a uma "caixa-preta" para ser acoplado ao robô Da Vinci com intuito de gravar a cirurgia. Este instrumento permite monitorar a posição dos dispositivos médicos e a maneira como o médico maneja o robô durante o procedimento cirúrgico. Facilmente, é possível observar se houve algum alerta ou sinal emitido pelo robô que foi ignorado pelo médico que

decidiu continuar a cirurgia assumindo o risco, considerando-se um serviço essencialmente médico como entende Nogaroli (2023).

É necessário estabelecer a "relação de correlação entre a violação do dever (ilicitude) por parte do médico e o dano (nexo de ilicitude)". (Nogaroli, 2023, p.153) A responsabilidade decorrerá principalmente da violação do direito do paciente à autodeterminação e à escolha, permitindo-lhe decidir de maneira livre e esclarecida sobre os riscos que deseja assumir ao comparar as possíveis alternativas de tratamento.

O dever de informação refere-se à obrigação dos profissionais de saúde de fornecer informações completas, claras e precisas aos pacientes sobre diagnósticos, tratamentos, riscos e alternativas disponíveis. Esta transparência é fundamental para que os pacientes possam tomar decisões informadas sobre seu cuidado e consentir com os procedimentos médicos de maneira consciente.

Além disso, a comunicação eficaz entre médicos e pacientes é essencial para estabelecer um nexo causal claro em casos de erro médico. Quando os pacientes são adequadamente informados, a identificação de falhas no processo de cuidado torna-se mais evidente, permitindo que se atribuam responsabilidades de maneira justa e precisa. Isso não só promove a justiça e a *accountability* no sistema de saúde, mas também contribui para a melhoria contínua da prática médica, reduzindo a incidência de erros e aumentando a segurança do paciente.

Dessa forma, no próximo tópico será analisado o dever de informação no contexto médico, destacando a importância do seu papel na prevenção de erros e danos aos pacientes.

3.3.1 Do dever de informação

A crescente utilização dos meios digitais por toda sociedade e dos mecanismos inteligentes autônomos em diversas áreas, como indústria, saúde, transporte e comunicações demandam a necessidade de melhor informação, transparência e segurança. Os usuários também têm o direito de serem informados sobre como as decisões são tomadas por sistemas de IA, na medida que essas decisões podem afetar aspectos importantes de suas vidas. A transparência sobre as capacidades e limitações das máquinas inteligentes é essencial para evitar danos e expectativas irreais.

No caso de uma cirurgia robótica, se o paciente não recebe informações adequadas e suficientes sobre o procedimento robótico cirúrgico e sobre o pós-operatório, ele não poderá dar um consentimento informado e, portanto, não terá a capacidade de proteger seus próprios

interesses.

Não obstante, com elevação da autodeterminação informativa, objetiva-se justamente a atribuição, ao paciente, da inexorável liberdade para que direcione os sentidos do seu tratamento médico. Dessa forma, o Código de Defesa do Consumidor (CDC) prevê a boa-fé. No contexto das operadoras de plano de saúde, o dever de informação e a boa-fé qualificada têm sido temas centrais em diversas decisões judiciais.

O Superior Tribunal de Justiça (STJ) já se posicionou claramente sobre a responsabilidade das operadoras de plano de saúde em cumprir uma boa-fé qualificada, que engloba os deveres de informação, cooperação e cuidado com o consumidor/segurado. Conforme decidido no Recurso Especial 418.572/SP, relatado pelo Ministro Luis Felipe Salomão, as operadoras devem atuar de maneira transparente e responsável, garantindo que os consumidores recebam todas as informações necessárias para tomar decisões informadas sobre seu tratamento e cobertura de saúde (DJe de 30.03.2009).

Esse entendimento é reforçado pelo voto da Ministra Nancy Andrighi no Recurso Especial 1.144.840/SP, que destaca a importância do dever de informação como um pilar fundamental na relação entre operadoras de plano de saúde e seus beneficiários. A boa-fé qualificada exige que as operadoras não apenas forneçam informações precisas e claras, mas também que cooperem de maneira ativa com os segurados, ajudando-os a entender seus direitos.

O entendimento claro dos impactos e responsabilidades associados a cada tipo de IA é essencial para moldar um futuro onde a inteligência artificial não apenas aprimora, mas também preserva os valores fundamentais da sociedade.

Na cirurgia assistida por robôs ou em procedimentos com suporte de inteligência artificial, assim como em outras intervenções médicas, o dever de informar é considerado um componente essencial. A não observância desse dever, decorrente da boa-fé objetiva do médico, configura um inadimplemento contratual. A indenização, nesse contexto, é devida pela privação da autodeterminação do paciente, privando-o da oportunidade de ponderar sobre os riscos e benefícios do tratamento (Nogaroli, 2023).

Para estabelecer a responsabilidade civil, é necessário analisar o nexo causal entre a omissão da informação e o dano sofrido pelo paciente. Mesmo quando a intervenção médica é tecnicamente correta, a falta ou inadequação da informação configura um elemento de culpa. Não é exigida negligência no tratamento; no entanto, a vítima deve demonstrar que o dano resultou de um risco que deveria ter sido comunicado, permitindo uma decisão informada sobre o tratamento (Nogaroli, 2023).

Nem todos os hospitais estão equipados com robôs cirúrgicos devido ao seu alto custo. Neste caso, na ausência de um robô, e se uma operação assistida por robô tiver maiores benefícios para o paciente, parece fundamental que o médico informe o paciente, ou até mesmo encaminhe o paciente para um hospital que o tenha. Parece concebível que um paciente culpe o médico por não fornecer essas informações antes da operação. No entanto, se o hospital tiver um robô cirúrgico, o médico deve oferecer ao paciente o melhor cuidado possível. Se uma operação assistida por robô tiver maiores benefícios para a saúde do paciente, então o médico deve recorrer à cirurgia robótica, provando que os avanços na robótica cirúrgica estão impactando os padrões de erro médico (Nogaroli, 2023).

A moderna dogmática da responsabilidade médica destaca o consentimento como um instrumento vital para respeitar a autonomia do paciente. Esse direito permite que o paciente, exercendo sua liberdade, escolha entre tratamentos apresentados, ou até mesmo opte por não realizar nenhum deles.

A adoção crescente de tecnologias na cirurgia, como a robótica e a inteligência artificial, ressalta a importância da ética, transparência e responsabilidade na prática médica. A integração desses avanços exige um cuidado especial com o dever de informar, reconhecendo a autonomia do paciente e assegurando que a inovação tecnológica não comprometa os princípios fundamentais da medicina e da responsabilidade civil.

Assim como os motoristas, os cirurgiões precisam adquirir habilidades para se movimentar em seus ambientes específicos, o que pode parecer simples em teoria, mas é incrivelmente complexo na prática. Os caminhos da vida real estão repletos de tráfego, equipamentos de construção, pedestres - elementos que nem sempre estão mapeados no Google Maps e que o cirurgião deve aprender a contornar (Gaines, 2022).

Da mesma forma, embora os corpos humanos possam ser geralmente semelhantes, as dimensões e formas exatas dos órgãos, a presença de tecido cicatricial e a disposição dos nervos ou vasos sanguíneos frequentemente variam de pessoa para pessoa (Nogaroli, 2023).

Usar um robô inteligente capaz de se dirigir sozinho tornaria uma colonoscopia que requer a passagem de um tubo flexível com uma câmera – um endoscópio – através do intestino para procurar sinais precoces de câncer de cólon, muito mais fácil – como dirigir um carro em um videogame. O médico poderia então se concentrar no assunto em questão: detectar os primeiros sinais de câncer. E neste caso, o robô, criado a partir de materiais macios, seria inerentemente mais seguro do que dispositivos mais rígidos. Pode até reduzir a necessidade de anestesia ou sedação, uma vez que poderia evitar mais facilmente empurrar as paredes intestinais. E como o robô não tem como cortar ou destruir nada sozinho, pode ser

mais fácil para os reguladores aceitarem esse tipo de cirurgia realizada por robô (Gaines, 2022).

Diante desse contexto inovador, surgem questões sobre os riscos do desenvolvimento tecnológico que serão melhores abordadas no próximo tópico.

3.4 TEORIA DO RISCO DO DESENVOLVIMENTO

A disseminação dos dispositivos tecnológicos, que se tornaram uma parte integral do nosso dia a dia, desempenha um papel de extrema importância na sociedade moderna. O avanço das tecnologias generativas, que se referem a capacidade de criar ou gerar continuamente novas capacidades, aplicações ou inovações, como a inteligência artificial (IA), o aprendizado de máquina e o *blockchain*, trouxe desafios e complexidades adicionais para o domínio da responsabilidade civil.

Surge, deste modo, a questão a ser enfrentada: Como estabelecer bases jurídicas ou impor limites legais às incertezas provenientes do ambiente tecnológico, sem perder de vista o desenvolvimento responsável e ético das tecnologias, o estímulo à pesquisa e a gestão de riscos? Importante, também, questionar os possíveis riscos que a sociedade moderna enfrenta com os cenários trazidos pela "convulsão tecnológica". Novas tecnologias geram novos riscos e por isso a necessidade de proteção e regulamentação.

Nesse contexto, o direito contemporâneo se ajusta e estabelece um quadro que incorpora os riscos e as inovações tecnológicas como componentes de um processo social no qual está imerso. Como é amplamente reconhecido, o direito evolui junto com a sociedade e, assim, tem conseguido se adaptar às suas necessidades em constante mudança. Isso nos leva a identificar, segundo o autor José Rubens Morato Leite, pelo menos três tipos de riscos, especificamente:

> "a) Riscos com dimensões planetárias, como o uso irracional da madeira, recursos minerais e outros;
> b) Riscos que não revelam situações de excepcional gravidade, como a erosão;
> c) Riscos invisíveis e anônimos, aqui cita-se o hiper-aquecimento da camada de ozônio que causa o efeito estufa, que apesar de invisível, constitui grande risco para a humanidade". (LEITE, p. 28)

A governança do risco ganha contornos dramáticos na atualidade e, consequentemente, é necessário buscar instrumentos que permitam o seu tratamento. Assim, o que não pode prescindir em relação a tecnologia é a análise e gestão de riscos, através de *compliance*, ou seja, a atuação em conformidade a estruturas bem delimitadas, revelando a expectativa de adesão a parâmetros regulatórios.

A noção de *compliance*, tradicionalmente associada à definição de parâmetros de governança em atividades públicas e à mitigação de riscos (Faleiros Júnior, 2022), tem evoluído para se tornar um elemento fundamental também no setor privado. Portanto, a gestão de riscos assume uma real importância nos dias de hoje, e, por conseguinte, torna-se imperativo procurar ferramentas que viabilizem sua abordagem por meio da prevenção legal (Viola, 2022).

A partir do desenvolvimento da humanidade e da evolução das gerações dos direitos fundamentais ao longo de décadas, nota-se uma expansão da abordagem e da prevenção de riscos no contexto legal. Começando essa análise pela Constituição Federal, é evidente que esta assegura o desenvolvimento econômico em seu artigo 170, caput, inciso VI. Além disso, o art. 196 da CF/88 assegura que o direito à saúde é garantido "mediante políticas sociais e econômicas que visem à redução do risco de doença e de outros agravos" (Brasil, 1988), tal dispositivo é reproduzido no art. 2º, § 1º, da Lei nº 8.080/90[5]. Dessa forma, a redução de riscos de "outros agravos" significa prevenir seus acontecimentos.

Os recentes desenvolvimentos tecnológicos constituem um cenário favorável à renovação dos debates doutrinários, jurisprudenciais e legislativos sobre a temática dos riscos do desenvolvimento tecnológico. Referindo-se à jurisprudência do Tribunal Constitucional da Alemanha, Mendes (2015) afirma que o Estado tem a obrigação de implementar ações de proteção aos cidadãos ou medidas preventivas em face do avanço técnico e tecnológico. Essa obrigação está associada ao "dever de evitar riscos", que surge do princípio que proíbe a proteção inadequada dos direitos fundamentais, particularmente os direitos sociais (Mendes, 2015, p. 641).

Uma abordagem fascinante para situar a responsabilidade civil envolve a utilização do conceito de "sociedade de risco", introduzido nos anos de 1980 por Ulrich Beck. O autor argumenta que a ciência e a tecnologia contemporâneas deram origem a uma sociedade caracterizada pelo risco, na qual a ênfase na geração de riqueza foi superada pela produção de riscos. Assim, o autor descreve uma sociedade em que os riscos estão cada vez mais ligados à atividade humana e tecnológica (Beck, 2011).

Ótica interessante trazida pelo sociólogo Ulrich Beck é o conceito sociológico de "modernidade reflexiva", que se referee a uma fase da modernidade em que a sociedade se torna cada vez mais consciente dos efeitos colaterais e das consequências não intencionais das

[5] Art. 2º A saúde é um direito fundamental do ser humano, devendo o Estado prover as condições indispensáveis ao seu pleno exercício. § 1º O dever do Estado de garantir a saúde consiste na formulação e execução de políticas econômicas e sociais que visem à redução de riscos de doenças e de outros agravos e no estabelecimento de condições que assegurem acesso universal e igualitário às ações e aos serviços para a sua promoção, proteção e recuperação.

ações humanas, especialmente aquelas relacionadas à ciência, tecnologia e economia. Nessa fase, as pessoas começam a questionar e refletir sobre as implicações de suas escolhas e ações, reconhecendo que as soluções para os problemas que enfrentam muitas vezes geram novos desafios (Beck, 2011).

A modernidade reflexiva é caracterizada por uma crescente ênfase na incerteza, na complexidade e na interconexão global, e leva a uma maior conscientização sobre questões ambientais, sociais e éticas. Essa abordagem reflexiva desafia as noções tradicionais de autoridade e conhecimento, dando lugar a uma maior participação e debate público sobre questões de grande importância, como o meio ambiente, a política, a ética e a responsabilidade individual e coletiva (Beck, 2011).

Portanto, a modernidade reflexiva se traduz na aspiração iluminista de uma racionalidade científica que se separa de uma racionalidade social prejudicial, forçada a se adaptar devido à ameaça da qual nenhum esforço permite se esquivar (Rosenvald; Braga Netto, 2024).

Diante do reconhecimento das dificuldades inerentes da sociedade moderna, caracterizada como uma sociedade de risco e impregnada pela cultura da incerteza, surgem desafios para atender à necessidade de uma prestação jurisdicional adequada e eficaz em relação aos direitos difusos, coletivos e individuais homogêneos. A questão atual é saber se o ordenamento jurídico brasileiro está preparado para proteger apropriadamente as pessoas perante uma gigantesca quantidade de novos riscos.

Nesta conjuntura, os riscos resultantes de inovações tecnológicas, fontes inestimáveis de uma variedade alarmante de acidentes, agravados pela crescente dificuldade, muitas vezes, de se comprovar a causa do incidente e a culpa do autor do ato ilícito, levaram a uma mudança significativa na tradicional teoria da culpa. Isso ocorreu com o propósito de concretizar a responsabilidade, demonstrando de maneira concreta e vivida que o Direito é, antes de tudo, uma disciplina derivada da vida real e destinada a regular essa própria vida (Lima, 1998, p.16).

Assim, a modernização reflexiva introduz um elemento inovador: a ciência se depara com as consequências e desafios gerados por sua própria inovação. A mudança na abordagem do risco leva em conta os progressos tecnológicos que têm um impacto significativo na sociedade, sobretudo a partir da segunda metade do século XVIII, e que adquirem uma nova magnitude no final do século XX (Viola, 2022, p. 27).

Na linha dos estudos realizados pelo autor Rafael Viola, os novos riscos exibem cinco principais características: (i) abrangência transfronteiriça, uma vez que esses riscos

ultrapassam fronteiras setoriais, sociais, nacionais e culturais, podendo se originar em um país ou setor específico e, em seguida, se espalham para outras áreas e setores; (ii) efeitos globalizantes, já que esses riscos tendem a afetar a todos e, com frequência, resultam em danos irreversíveis; (iii) poder penetrante ampliado, pois esses riscos têm a capacidade de penetrar e transformar significativamente sistemas sociais e culturais, modificando o comportamento social, como no caso dos organismos geneticamente modificados na agricultura; (iv) natureza incalculável, devido à falta de fronteiras e às complexas consequências globais associadas à tomada de riscos, levando a inadequações e imprecisões nos instrumentos e ferramentas para avaliar esses riscos, tornando difícil até mesmo para as seguradoras calcular prêmios proporcionais aos riscos envolvidos; e (v) ausência de responsabilização (*accountability*), uma vez que as potenciais vítimas desses riscos têm sido sobrecarregadas sem seu consentimento, sem que qualquer pessoa ou instituição seja por isso responsabilizada (Viola, 2022).

Dada a rápida e incerta taxa de mudança na área de IA, e no contexto do aumento acelerado dos investimentos em tecnologia, ressalta-se a urgência de aprofundar nossa compreensão desses riscos potenciais e das medidas necessárias para enfrentá-los. Nesse contexto, surge a teoria do risco do desenvolvimento, de modo especial em casos envolvendo produtos defeituosos ou danos causados por tecnologias inovadoras.

A teoria do risco do desenvolvimento prevista no Código de Defesa do Consumidor (CDC) consiste na ideia de que o fornecedor não tinha conhecimento, nem motivo para conhecer, dos perigos do produto ao introduzi-lo no mercado de consumo, somente vindo a conhecer após avanços tecnológicos (Braga Netto, 2024). À vista disso, o CDC estatui: “Art. 10. O fornecedor não poderá colocar no mercado de consumo produto ou serviço que sabe ou deveria saber apresentar alto grau de nocividade ou periculosidade à saúde ou segurança” (Brasil, 1990)

Já o § 1º dispõe,

> “O fornecedor de produtos e serviços que, posteriormente à sua introdução no mercado de consumo, tiver conhecimento da periculosidade que apresentem, deverá comunicar o fato imediatamente às autoridades competentes e aos consumidores, mediante anúncios publicitários”.

Ademais, a “época em que foi colocado em circulação” deve ser verificada para se considerar, ou não, determinado produto defeituoso (art. 12, § 1º, III), lembrando que o produto não é reputado defeituoso em razão de outro, de qualidade superior, ter sido colocado no mercado (CDC, art. 12, § 2º) (Brasil, 1990).

Assim, pode-se dizer que aquela teoria é aplicada quando um dano ocorre devido a um

defeito que era desconhecido no momento da fabricação ou distribuição do produto, e que não poderia ser detectado com o conhecimento científico e tecnológico disponível naquele tempo. Isso implica que o fabricante pode ser responsável mesmo que tenha observado todas as normas de segurança e não tenha como prever o defeito naquele momento.

Alguns argumentam que a teoria do risco do desenvolvimento pode funcionar como uma cláusula de exclusão de responsabilidade para os desenvolvedores das inteligências não naturais. Essa perspectiva sugere que, se eles empregaram a tecnologia mais avançada disponível na época, o subsequente surgimento de inovações mais recentes e seguras não deveria implicar em falhas da IA. Assumir responsabilidade nesse contexto seria uma penalização excessiva, especialmente considerando que os supostos defeitos não seriam detectáveis pelo fabricante (Tepedino; Silva, 2019).

O risco do desenvolvimento tecnológico pode ser entendido como uma

> [...] expressão que busca aludir à possibilidade de que o desenvolvimento científico venha a apresentar novas e mais seguras tecnologias que anteriormente não poderiam ser conhecidas pelo agente, o que justificaria a exclusão da sua responsabilidade por eventuais danos (Tepedino; Silva, 2019, p. 78).

Dessa maneira, o risco do desenvolvimento, portanto, se refere aos danos provocados por um produto que, inicialmente, não apresenta defeitos evidentes. Isso ocorre devido a não capacidade técnica de detectar ameaças e danos no momento em que o produto é lançado no mercado, somente sendo verificados após avanços científicos subsequentes.

Nessa perspectiva, diante das questões relativas às previsões dos riscos e incertezas científicas, a concepção de risco do desenvolvimento surge como um elemento que, em certas ocasiões, é mencionado como um impedimento para atribuir responsabilidade. Os riscos do desenvolvimento referem-se aos impactos adversos secundários que tem potencial de acontecer após esses produtos terem sido disponibilizados aos consumidores (Menezes; Coelho; Bugarim, 2011).

De acordo com o artigo 7º, alínea "e" da Diretiva da Comunidade Europeia (Diretiva 85/374/CEE), o fabricante não será responsabilizado conforme a legislação vigente se demonstrar que, no momento em que o produto foi lançado ao mercado, o nível de conhecimento científico e técnico existente não possibilitava a identificação do defeito no produto.

Relembrando as discussões ocorridas na União Europeia, quando da aprovação da Diretiva 85/374, a definição de risco do desenvolvimento envolvia os seguintes pontos: a) funda-se na responsabilidade civil objetiva; b) consagra o risco do desenvolvimento como causa excludente da responsabilidade civil; c) para ser admitida essa excludente, o

produtor tem o ônus de provar que, no momento da colocação do produto no mercado, não era possível detectar a existência do defeito; d) a legislação interna de cada Estado-membro pode ou não incorporar a excludente do risco do desenvolvimento; e) o critério temporal para aferição do estado da ciência e da técnica ou estado da arte é o da colocação do produto no mercado e não o da verificação do dano (Braga Netto, 2024). Assim, na Europa o risco do desenvolvimento é causa de exclusão da responsabilidade civil.

Na visão de Braga Netto o risco do desenvolvimento diz respeito a danos causados por produtos que no momento da sua disponibilização mercantil,

> [...] não se podia cientificamente saber que eram perigosos, considerando-se o estado atual da ciência e da técnica. Importante frisar que essa incognoscibilidade é absoluta e não relativa. Em outras palavras, não é para esse ou aquele fornecedor, mas para todos. (Braga Netto, 2024, p. 5)

Em relação a riscos considerados muito elevados, ou seja, com uma alta probabilidade de ocorrência e previsibilidade em relação a danos significativos, é crucial exercer extrema cautela em relação ao denominado *"sandbox"*. Trata-se de uma adaptação de um conceito computacional para o ambiente jurídico regulatório, que disponibiliza espaços experimentais concedendo "descontos regulatórios" em relação ao corpo normativo existente, desde que sob supervisão autorizada (Santana; Meirelles, 2022, p. 24).

Além disso, é importante destacar, concordando com a ponderação do Parlamento Europeu na Resolução que regulamenta a responsabilidade civil no ano de 2020, que a responsabilidade civil do operador deve ser aplicada a todos os tipos de operações de sistemas de Inteligência Artificial. Isso é válido independentemente da localização da operação e se é de natureza física ou virtual, essencialmente devido à natureza arriscada da atividade.

Esses riscos são potencializados ainda mais quando a operação ocorre em um espaço público, colocando muitas pessoas em perigo. Isso ocorre porque as potenciais vítimas de lesões ou danos frequentemente desconhecem a exposição ao perigo e, geralmente, não têm a capacidade de iniciar uma ação de responsabilidade contratual contra o operador (Braga Netto, 2024).

É recomendável recordar que o Superior Tribunal de Justiça (STJ) em uma decisão de grande importância (REsp 1.774.372, julgado em 2020), abordou a teoria do risco do desenvolvimento. O tribunal deliberou de maneira apropriada, indicando que os ônus relacionados aos riscos recaem sobre o fornecedor, não sobre o consumidor ou o cidadão. O STJ ressaltou

> O risco do desenvolvimento, compreendido como aquele que não podia ser conhecido ou evitado no momento em que o medicamento foi disponibilizado, configura um defeito presente desde a concepção do produto, mesmo que não seja

> perceptível a priori, caracterizando, assim, uma situação de fortuito interno (STJ, 2020).

Portanto, no Brasil, o fornecedor de produtos e serviços é responsável pela teoria do risco do desenvolvimento, não sendo esta uma exclusão de responsabilidade civil em nosso sistema.

4 PREVENÇÃO E GESTÃO DOS RISCOS NO DESENVOLVIMENTO DA INTELIGÊNCIA ARTIFICIAL

A inteligência não natural tem sido cada vez mais utilizada em diversas áreas, desde assistentes virtuais em *smartphones* até sistemas de diagnóstico médico, cirurgiões robóticos e carros autônomos. Os perigos decorrentes das inovações tecnológicas, que frequentemente dão origem a uma ampla gama de acidentes imprevisíveis, têm sido agravados pelo crescente desafio de estabelecer a causa desses incidentes e a culpabilidade do agente responsável. Isso resultou em uma mudança significativa, evidenciando de forma concreta que o Direito é, em última instância, uma disciplina derivada da vida real destinada a regulamentar essa mesma realidade.

O perigo de mau funcionamento não se limita apenas a potenciais incidentes resultantes de uma condução automatizada inadequada. Isso também abrange, por exemplo, a falta de proteção adequada contra operações de hackers, que se tornaram uma das principais ameaças à medida que a mecatrônica e a automação inteligente se expandem no contexto dos carros autônomos. Além disso, diz respeito à questão das violações de privacidade, à medida que os sistemas de direção se tornam cada vez mais monitorados e rastreados (Ruffolo, 2017).

Os novos riscos apresentam características como abrangência transfronteiriça, efeitos globalizantes, poder penetrante ampliado, natureza incalculável e ausência de responsabilização (Viola, 2022). O conceito de risco pode ser entendido como a simples probabilidade de ocorrer algum dano. No entanto, a presença de risco por si só não é suficiente para justificar uma obrigação de indenização. É necessário que o dano efetivamente ocorra. Além disso, a existência de um risco acarreta a responsabilidade de garantir segurança, implicando um dever de proteção contra possíveis prejuízos. Melo e Cardoso (2022) destacam a necessidade de adaptação dos sistemas jurídicos para lidar com os desafios impostos pela IA, especialmente em casos de danos causados por esses sistemas.

Ao mesmo tempo em que a tecnologia traz inúmeros benefícios e está enraizada nos Estados, é necessário ponderar sua utilização e o momento econômico pelo qual o mundo passa, pois observa-se os novos riscos e conflitos sociais que emergem da exploração de tecnologias digitais.

É necessário observar às transformações tecnológicas, pois as sociedades tendem a se dividir em círculos fechados ou bolhas informativas, entre novas segregações, e tribos identitárias. O sociólogo espanhol Manuel Castells traz a ideia de que há uma tendência dos

processos dominantes na era da informação de se organizar em torno de redes da internet, e a difusão da lógica nessas redes modifica de forma significativa a operação e os resultados dos processos produtivos, da experiência, das relações de poder e da cultura (Castells, 2013).

Castells também expõe que uma das características centrais da sociedade em rede é essa transformação no campo das comunicações, incluindo as mídias. Segundo ele, a comunicação constitui o espaço público, ou seja, o espaço cognitivo em que as mentes das pessoas recebem informação e formam os seus pontos de vista, processando os sinais da sociedade. É por essa razão que a estrutura e a dinâmica da comunicação social são essenciais para a formação da consciência e da opinião e ainda a base do processo de hiperconexão (Castells, 2013, p.565-573).

Entende-se por hiperconexão, a intensificação e expansão das redes de comunicação, especialmente a internet, que têm transformado profundamente a maneira como as pessoas se relacionam, trabalham e se informam, justamente pela utilização dos algoritmos. Assim, as IA desempenham um papel fundamental na disseminação de informações, moldando o que as pessoas veem em suas redes sociais e plataformas de notícias.

Essa interconexão é um elemento central na sociedade contemporânea, reconfigurando as relações sociais e criando novas formas de interação. Em sua análise, Castells destaca que a hiperconexão não se trata apenas de uma questão tecnológica, mas sim de um fenômeno que permeia todos os aspectos da vida. As redes não apenas facilitam a comunicação, mas também influenciam a formação de identidades, o poder político, a economia e até mesmo a estruturação do tempo e do espaço.

Com isso, as interações entre as pessoas e as tecnologias são constantes. Algoritmos são responsáveis por otimizar e personalizar experiências online, adaptando conteúdos e recomendações com base no comportamento e preferências individuais.

A crescente dependência de sistemas interconectados expõe a sociedade a vulnerabilidades que necessitam da construção de normativas que possam prevenir e reparar os danos perpetrados pelo desenvolvimento tecnológico. Executivos das grandes empresas tecnológicas e líderes políticos têm alertado que o avanço rápido dos sistemas inteligentes representa uma ameaça existencial global se não for devidamente controlado. Isso desencadeou uma corrida entre governos e organizações internacionais a fim de estabelecer salvaguardas e regulamentações (Pires; Silva, 2017).

Nesse sentido, a China, os Estados Unidos, Brasil, e mais 25 países estão trabalhando no gerenciamento coletivo dos riscos gerados pelas inteligências não naturais a fim de trilhar um caminho seguro para a tecnologia (Sandle; Coulter, 2023).

Assim, em uma ação sem precedentes no contexto dos esforços ocidentais para supervisionar o desenvolvimento seguro da IA, um vice-ministro chinês colaborou com autoridades dos EUA e da UE, bem como com presidentes de empresas de tecnologia notáveis, como Elon Musk, da X (antigo Twitter), e Sam Altman, do OpenAir (ChatGPT). Esse encontro ocorreu no Bletchley Park, local histórico onde foi o centro dos decifradores de códigos durante a Segunda Guerra Mundial, no Reino Unido (Sandle; Coulter, 2023).

O encontro daqueles líderes proporcionou a assinatura da Declaração de Bletchley, documento pelo qual afirmaram o compromisso de trabalharem em conjunto para o estabelecimento de uma abordagem comum de supervisão. Tal declaração delineou uma agenda dual, concentrando-se na identificação de riscos de preocupação mútua e na construção de um consenso científico sobre essas questões, uma vez que muitos dos riscos associados à inteligência não natural são intrinsecamente de natureza internacional e, portanto, são mais eficazmente abordados por meio da cooperação internacional.

Além disso, o acordo firmado propôs o desenvolvimento de políticas colaborativas entre os países com o objetivo de reduzir aqueles riscos (Sandle; Coulter, 2023), sendo destacada a necessidade de os países considerarem a importância de uma governança e abordagem regulatória pró-inovação e proporcionada, maximizando os benefícios e levando em consideração os riscos associados à IA.

Isso pode incluir a elaboração, quando apropriado, de classificações e categorizações de risco, adaptadas às circunstâncias nacionais e aos enquadramentos legais pertinentes. Foi destacado também a pertinência da cooperação em abordagens como princípios comuns e códigos de conduta, quando apropriado.

Em relação aos riscos específicos mais provavelmente encontrados em relação à IA de fronteira, que são modelos altamente capazes de uso geral, decidiram os países na Declaração de Bletchley intensificar e manter a cooperação, estendendo-a a outros países. O objetivo é identificar, compreender e, conforme apropriado, agir, por meio de fóruns internacionais existentes e outras iniciativas relevantes, incluindo futuras Cúpulas Internacionais de Segurança de IA[6].

Nessa linha de preocupação acerca do uso de ferramentas de IA, o Conselho Nacional do Ministério Público – CNMP propôs, recentemente, recomendação para a utilização de sistemas de inteligências no âmbito do Ministério Público brasileiro. Conforme a recomendação, o aperfeiçoamento, a concretização e a utilização de ferramentas de IA

[6] Informação constante do site https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023. Acesso em: 19 nov. 2023.

generativa devem observar princípios, dentre outros, como a:

> centralidade da pessoa humana; o respeito aos direitos humanos e aos valores democráticos; a igualdade e não discriminação; o fomento ao desenvolvimento tecnológico e à inovação responsável; a privacidade, segurança, proteção de dados e autodeterminação informativa (OAB, 2023).

A referida recomendação, também, destaca a necessidade de impulsionar treinamentos e conscientização sobre o uso desses dispositivos digitais, visando uma aplicação efetiva e protegida. A sensibilidade dos dados manuseados levanta preocupações sobre vazamentos, uso indevido e exposição de informações privadas durante o treinamento de modelos de IA. Outrossim, propõe monitoramento e revisão periódicos para se adaptar às mudanças da tecnologia e da legislação. A norma orienta, ainda, que as instituições promovam um ambiente digital propício à IA, e assegurem investimentos em infraestrutura digital, pesquisa e desenvolvimento da IA (Migalhas, 2023).

Desse modo, se faz necessário compreender os limites, as vulnerabilidades e as possíveis consequências do uso inadequado de tecnologias inteligentes para a tomada de decisões informadas. Nessa perspectiva, a diversidade de tipos de IA reflete não apenas a evolução técnica, mas também a necessidade de uma abordagem ética e jurídica cuidadosa. Assim, o presente capítulo buscou analisar as estratégias adotadas pelos Estados Unidos e pela União Europeia para prevenir e gerenciar os riscos e os possíveis perigos associados ao uso das novas descobertas científicas.

4.1 GERENCIAMENTO DE RISCOS DA IA PELAS NORMATIVAS DOS ESTADOS UNIDOS

O gerenciamento dos riscos pela utilização das inteligências não naturais nos Estados Unidos da América começou a partir do *Algorithmic Accountability Act* (AAA) de 2019. O *Algorithmic Accountability Act* (Lei de Responsabilidade Algorítmica) é uma proposta de legislação nos Estados Unidos que visa abordar as preocupações crescentes em torno da utilização enorme de sistemas de decisão automatizados – *automated decision systems* (ADS). Apresentado pelos senadores Ron Wyden, Cory Booker e pela deputada Yvette D. Clarke, o projeto procura estabelecer diretrizes e regulamentos para garantir transparência e responsabilidade na implantação de algoritmos, especialmente em áreas que impactam a vida dos indivíduos (Chatterje; Kern, 2023).

As principais disposições da Lei de Responsabilidade Algorítmica incluem a exigência de que as empresas realizem avaliações de impacto em sistemas de decisão

automatizados, comumente chamados de algoritmos, que impactam significativamente a privacidade do consumidor, os direitos civis ou resultam em resultados díspares. Estas avaliações de impacto destinam-se a avaliar os potenciais preconceitos, discriminação e outros efeitos adversos dos algoritmos em diferentes grupos demográficos (Rosenvald, 2023).

O AAA sugere que as entidades que incorporam esses sistemas adotem diversas medidas concretas para reconhecer e reduzir os riscos sociais, éticos e legais. Como uma iniciativa normativa para supervisionar os algoritmos em todas as áreas, o AAA dos Estados Unidos representa um ponto de referência em uma disposição global de complementar ou substituir a autorregulação neste campo por meio de legislação, a exemplo da proposta de Lei de Inteligência Artificial pela Comissão Europeia em 2021 (Rosenvald, 2023).

Além disso, a Lei de Responsabilidade Algorítmica visa a aumentar a transparência, garantindo que os indivíduos afetados sejam informados sobre a utilização de sistemas de decisão automatizados e tenham o direito de aceder às informações utilizadas nesses sistemas. Nesse sentido, a cidade de Nova Iorque adotou a Lei nº 1.696-A/2017, visando assegurar a transparência dos algoritmos empregados pelo setor público, especificando o que constitui um sistema de decisão automatizado:

> [...] implementações computadorizadas de algoritmos, incluindo aqueles que derivam de técnicas de aprendizado de máquina ou outras tecnologias de processamento de dados ou inteligência artificial, utilizados para auxiliar na tomada de decisões. (Silva, 2021, p. 45).

A referida lei foi elaborada para fornecer aos indivíduos maior controle sobre seus dados pessoais e promover a responsabilização entre as empresas que implantam algoritmos (Silva, 2021). Portanto, pode se dizer que esse controle de parâmetros regulatórios preventivos se concretiza por meio da *accountability*.

O AAA americano orienta todas as agências sob sua supervisão a monitorar a competição empresarial na área da inteligência artificial, observando atentamente os "riscos decorrentes do controle concentrado" e evitando que as empresas multimilionárias dominantes consolidem ainda mais o poder. Há uma preocupação crescente de que apenas as maiores empresas, como Google, Apple, Amazon e Microsoft, possam competir de maneira eficaz (Chatterje; Kern, 2023, p. 2).

A legislação proposta reflete um reconhecimento crescente da necessidade de quadros regulamentares para acompanhar o rápido avanço da IA e das tecnologias algorítmicas. Ao abordar os potenciais riscos e preconceitos associados à tomada de decisões algorítmicas, a Lei de Responsabilidade Algorítmica procura encontrar um equilíbrio entre a inovação e a proteção dos direitos e da privacidade dos indivíduos afetados por estes sistemas.

Dessa forma, o *Algorithmic Accountability Act* 2022 é uma declaração de ética na implantação dos projetos de inteligência artificial, ou seja, é um conjunto de diretrizes para eliminar ou ao menos mitigar os impactos negativos causados pela introdução de algoritmos. Fundamenta-se na análise econômica do direito, uma vez que a *Law and the Economics* ensina que quem está numa posição hierárquica superior, quem pode fazer escolhas tem a obrigação de justificar as escolhas tomadas, bem como indicar, prevenir e mitigar os danos (Rosenvald; Braga Netto, 2024).

As IAs autônomas introduzem complexidades, uma vez que suas ações muitas vezes não são diretamente controladas por humanos. Assim, a autonomia da IA traz consigo o risco de reações imprevisíveis. Os riscos foram identificados como não intencionais e aparentemente intransponíveis, expondo toda a sociedade a uma possível condição de perigo (Tepedino; Silva, 2019). Como, então, abordar esse cenário que parece não ter solução?

Em resposta à escalada das capacidades da IA e ao seu consequente impacto na segurança e proteção dos americanos, os Estados Unidos emitiram uma Ordem Executiva que delineia as medidas mais abrangentes algumas vezes implementadas. Estas ações visam proteger os americanos dos riscos potenciais representados pelos sistemas de IA.

Nessa perspectiva, o presidente Biden assinou recentemente a Ordem Executiva em 30 de outubro 2023, estabelecendo diretrizes norte-americanas para o fim de desenvolver capacidades e impulsionar invenções de IA que sejam de interesse nacional. Ordens Executivas nos Estados Unidos são ações administrativas tomadas pelo Presidente para referenciar operações governamentais e implementar políticas. O governo dos EUA tem mostrado interesse em promover o desenvolvimento ético e responsável da IA. Utiliza-se o termo inteligência artificial para designar software automatizado com capacidades preditivas, perceptivas ou geradoras que podem imitar determinadas habilidades humanas.

As medidas implementadas alinham-se e complementam iniciativas como a liderança do Japão no Processo de Hiroshima do G-7, a Cimeira do Reino Unido sobre Segurança da IA, o papel da Índia como Presidente da Parceria Global sobre IA e os debates em curso nas Nações Unidas. As diretivas do presidente Biden representam avanços significativos na abordagem dos EUA para garantir uma IA segura, protegida e confiável. Embora sejam necessárias mais medidas, o governo americano está empenhado em trabalhar com o Congresso na prossecução de legislação bipartidária, reforçando a liderança da América na inovação responsável.

Essa mais recente ordem executiva leva os Estados Unidos a uma abordagem mais abrangente na governança da IA. Em contraste com medidas anteriores, esta vai além de

princípios e diretrizes, incluindo seções que impõem ações específicas tanto às empresas de tecnologia quanto às agências federais (Rosenvald, 2023).

No seu compromisso de promover o desenvolvimento responsável e a utilização da inteligência artificial, a Administração Biden está a tomar medidas decisivas, tanto a nível nacional como a nível internacional. Outrossim, planeja estabelecer várias agências federais para monitorar os riscos da IA e explorar novas aplicações para essa tecnologia, ao mesmo tempo em que busca proteger os trabalhadores. Também aborda o emprego da inteligência artificial no ambiente de trabalho, destacando a importância de não utilizar a tecnologia para incentivar a vigilância inadequada dos trabalhadores. A ordem também nomeará um Conselho de IA da Casa Branca para coordenar as atividades de IA do governo federal, presidido pelo Vice-Chefe de Gabinete de Política da Casa Branca e composto por representantes de todas as principais agências (Chatterje; Kern, 2023).

Baseada em uma "Declaração de Direitos" emitida pelo governo de Biden no final de 2022, que abordou muitas das preocupações levantadas por grupos da sociedade civil, a ordem acrescenta um impulso significativo para explorar também as capacidades da inteligência artificial, incluindo o lançamento do programa piloto de investigação pública conhecido como National AI Research Resource, ou NAIRR (Chatterje; Kern, 2023).

A referida diretiva norte-americana também autoriza Washington a monitorar o desenvolvimento do setor privado em relação aos poderosos sistemas de IA. Isso inclui um mandato para que as empresas apresentem relatórios ao governo federal detalhando como treinam e testam os chamados "modelos de base de dupla utilização", uma categoria que abrange os sistemas mais avançados de algoritmos (Chatterje; Kern, 2023).

Em nível interno, a Administração insta o Congresso a aprovar legislação bipartidária sobre privacidade de dados para proteger todos os americanos, com especial atenção para as crianças. A recente Ordem Executiva estabelece medidas inovadoras para garantir a segurança, a proteção e a fiabilidade dos sistemas de IA, incluindo a partilha obrigatória de resultados de testes de segurança e informações críticas por parte dos criadores de poderosos sistemas de IA com o governo dos EUA (Chatterje; Kern, 2023).

Para proteger a privacidade dos americanos, o Presidente apelou ao Congresso para aprovar uma legislação abrangente sobre privacidade de dados. A legislação proposta visa salvaguardar a privacidade de todos os cidadãos, especialmente das crianças, e inclui ações como a priorização do apoio federal para técnicas de preservação da privacidade e o reforço da investigação em tecnologias de preservação da privacidade. A ordem executiva estabelecerá salvaguardas de privacidade em torno dos dados que alimentam a maioria dos

sistemas de inteligência artificial, conforme delineado no AAA. E, ainda, estabelecerá diretrizes para mitigar os riscos de privacidade quando o governo coletar, usar, compartilhar e excluir informações adquiridas de banco de dados (Rosenvald, 2024).

Nesse sentido, a ordem de Biden estimula as agências federais a incorporarem tecnologia de última geração para aprimorar a privacidade na proteção dos dados que coletam. Além disso, insiste a National Science Foundation a financiar uma nova rede de pesquisa voltada para o desenvolvimento, avanço e implementação de tecnologia de privacidade destinada ao uso das agências federais (Chatterje; Kern, 2023).

Estas iniciativas envolvem a avaliação de como as agências governamentais recolhem e utilizam informações comercialmente disponíveis, com foco específico em dados de identificação pessoal. O objetivo é melhorar as orientações sobre privacidade para agências federais e desenvolver diretrizes para avaliar a eficácia das técnicas de preservação da privacidade, incluindo aquelas utilizadas em sistemas de IA (Chatterje; Kern, 2023).

De mais a mais, a Administração Biden está a colaborar ativamente com aliados e parceiros em todo o mundo para estabelecer um quadro internacional robusto para o desenvolvimento e utilização da IA. Foram realizadas extensas consultas com vários países, incluindo Austrália, Brasil, Canadá, Chile, União Europeia, França, Alemanha, Índia, Israel, Itália, Japão, Quênia, México, Países Baixos, Nova Zelândia, Nigéria, Filipinas, Singapura, Coreia do Sul, Emirados Árabes Unidos e Reino Unido (Chatterje; Kern, 2023).

Apesar de a ordem não possuir força legal e de críticas anteriores aos esforços de gerenciamento dos riscos dos sistemas inteligentes pela Casa Branca terem apontado para a falta de aplicabilidade, as novas diretrizes conferirão às agências federais influência no mercado dos EUA por meio de seu poder de compra e ferramentas de aplicação. A ordem de Biden instrui especificamente a Comissão Federal de Comércio (Federal Trade Commission - FTC) a focar em comportamento anticompetitivo e danos ao consumidor na indústria de IA (Chatterie; Kern, 2023).

É digno de nota que a ordem citada faz uma menção específica à FTC, a utilizar sua autoridade regulatória para fortalecer a concorrência no setor e proteger os interesses dos consumidores. Essa ordem representa o esforço mais significativo até o momento para impor uma ordem nacional a uma tecnologia que surpreendeu muitos com seu rápido crescimento, especialmente as capacidades equiparadas às humanas dos mais recentes e potentes modelos de inteligência artificial generativa (Chatterie; Kern, 2023).

Assim sendo, a ordem executiva, como tal, não é capaz de resolver todos os desafios apresentados pelo avanço da inteligência artificial, uma vez que é inerentemente limitada em

seu poder e facilmente reversível. Por essa razão, a própria ordem demanda o Congresso a promulgar legislação sobre privacidade de dados. No entanto, é inegável que representa um avanço significativo ao preencher uma lacuna política. Enquanto a União Europeia trabalha publicamente no desenvolvimento do EU AI Act, que está prestes a se tornar lei, os Estados Unidos ainda não conseguiram alcançar progressos parecidos. Com a ordem executiva, surgem esforços a serem trilhados e transformações no caminho a diante.

Os desafios complexos que demandam abordagem envolvem determinar quais modos de julgamento e evidências devem ser considerados legítimos – ou, pelo menos, socialmente aceitáveis – para diversos processos de tomada de decisão, tanto públicos quanto privados. Responder a essas questões requer uma perspectiva otimista sobre o que as sociedades futuras deveriam ser. Os políticos precisam transcender as tentativas de garantir apenas uma responsabilidade algorítmica mínima, direcionando seus esforços para a criação de mecanismos de governança pública que possibilitem às organizações alcançar engajamentos que possam ser justificados dentro das margens da legalidade (Rosenvald, 2024).

Dessa forma, a ordem executiva, embora não seja uma solução definitiva, representa um avanço significativo na abordagem dos impactos da IA sinalizando uma mudança no horizonte regulatório e incentivando esforços adicionais para lidar com os desafios em constante evolução tecnológica.

4.2 GERENCIAMENTO DE RISCOS DA IA PELAS NORMATIVAS DA UNIÃO EUROPEIA

A União Europeia (UE) destaca fortemente a importância de uma abordagem ética para a IA priorizando a transparência, explicabilidade e a proteção dos direitos individuais. O Regulamento Geral de Proteção de Dados – *General Data Protection Regulation* (GDPR) é um exemplo claro dessa ênfase na privacidade e na autonomia do indivíduo. Nos termos da Resolução do Parlamento Europeu 2015/2103 (INL), os pedidos de patentes para tecnologia robótica triplicaram ao longo da última década (Parlamento Europeu, 2017).

A Resolução do Parlamento Europeu, de 16 de fevereiro de 2017, com recomendações à Comissão de Direito Civil sobre Robótica (2015/2103-INL) visa conferir à União Europeia um papel pioneiro na formulação de princípios éticos fundamentais a serem observados no desenvolvimento, programação e na utilização de robôs e sistemas inteligentes, com a intenção de incorporar aqueles princípios nos regulamentos e na legislação de seus países (Pires; Silva, 2017). A referida comissão destaca que os robôs autônomos inteligentes são

assim considerados a partir das seguintes categorias, como delimitado por Pereira:

> a) aquisição de autonomia através de sensores e/ou da troca de dados com o seu ambiente (interconetividade) e da troca e análise desses dados; b) autoaprendizagem com a experiência e com a interação (critério opcional); c) um suporte físico mínimo; d) adaptação do seu comportamento e das suas ações ao ambiente; e e) inexistência de vida no sentido biológico do termo. (Pereira, 2019, p. 129)

Portanto, entre os assuntos mais relevantes que foram debatidos na resolução citada estão a proposta de criação de uma agência reguladora em nível europeu; regulamentação da elaboração de procedimentos de experimentação para teste dos novos modelos robóticos na área médica (Tepedino; Silva, 2019).

O objetivo, em boa parte, consiste em moldar os avanços tecnológicos, prevenindo, no que couber, possíveis riscos por meio de uma abordagem progressiva, pragmática e cautelosa (Pires; Silva, 2017). Essas abordagens refletem a complexidade e a interdisciplinaridade do tema, considerando o risco como um elemento importante na atribuição de responsabilidade.

A normativa da UE reflete a preocupação em moldar a revolução tecnológica de maneira cuidadosa e gradual, evitando potenciais riscos. A ênfase na integração de princípios éticos sugere a importância de considerações morais e sociais no desenvolvimento dessas tecnologias, visando não apenas a eficiência técnica, mas também a responsabilidade e a segurança. Entretanto, vozes como Ruffolo (2017) abordam a existência de lacunas na Resolução de 16/02/2017 no que diz respeito aos danos e indenizações relacionados as questões recentes trazidas pela inteligência artificial.

Neste aspecto, a própria resolução enumera explicitamente, o assunto relacionado à gestão dos danos provocados por múltiplos robôs intervenientes, quando não se pode identificar claramente o interveniente humano específico responsável (Parlamento Europeu, 2017).

Assim, a abordagem pragmática e cautelosa da UE indica um reconhecimento da complexidade e das implicações dessas inovações. Ao incorporar gradualmente os princípios éticos nos regulamentos, a UE busca equilibrar a promoção da inovação em harmonia às célebres Leis de Asimov. Para garantir que o avanço tecnológico ocorra de maneira ética e sustentável, a Comissão da UE tratou do princípio da precaução, ao dispor que: “a avaliação de riscos consiste em quatro componentes – designadamente, a identificação do perigo, a caracterização do perigo, a avaliação da exposição e a caracterização do risco”, de maneira que “os limites do conhecimento científico podem afetar cada uma destas componentes” (Santos, 2020, p. 15).

Apesar de a Comissão da União Europeia ter divulgado um comunicado detalhado e

técnico sobre o princípio da precaução, ela não estabeleceu uma diretriz clara a respeito. Inicialmente, menciona que, na maioria das situações, cabe aos consumidores e às associações que os representam demonstrar o risco associado a um produto ou procedimento disponibilizado no mercado, exceto para medicamentos, pesticidas e aditivos alimentares. No entanto, a Comissão considera que, em certos casos, pode ser necessário que o produtor, fabricante ou importador comprove que seu produto ou processo é seguro. Esta exigência deve ser avaliada individualmente, sem que possa ser aplicada de forma generalizada a todos os produtos e processos no mercado (Santos, 2020).

A UE destaca explicitamente a necessidade de abordar o viés algorítmico e a discriminação, enfatizando a importância de sistemas de IA imparciais. Medidas específicas, como Avaliações de Impacto Ético, são incentivadas para mitigar esses riscos. A Avaliação de Impacto de Privacidade é uma ferramenta fundamental para avaliar e mitigar riscos relacionados à privacidade (English; Doherty; Stiernet, 2023).

Nessa linha, ao buscar a cooperação internacional e endossar um papel importante para os padrões internacionais, a UE reconhece a necessidade de uma abordagem global no gerenciamento de riscos relacionados à IA. Isso não apenas fortalece a posição da UE como referência ética, mas também contribui para a criação de um ambiente regulatório coeso e harmonizado em escala global.

A legislação de inteligência artificial da União Europeia faz uma compreensão centrada no risco para os sistemas AAA (Autenticação, Autorização e Auditoria), utilizando a pirâmide de criticidade. A abordagem baseada em risco e as avaliações de impacto nos direitos fundamentais mencionadas na sigla AAA se referem a: **Autenticação**, que é a verificação da identidade de um usuário, garantindo que a pessoa ou entidade acesse um sistema a quem alega ser; **Autorização**, no que tange à determinação dos direitos e permissões de um usuário em um sistema, ou seja, quais ações específicas essa pessoa ou entidade está autorizada a realizar; e **Auditoria,** que trata do registro e monitoramento de atividade de usuários em um sistema e permite a análise posterior das ações realizadas (English; Doherty; Stiernet, 2023).

Ainda, cabe mencionar que a legislação está focada em normatizar sistemas de IA com potencial impacto significativo. Ela designa regras e responsabilidades específicas para fornecedores, importadores, distribuidores, implantadores e representantes autorizados, com base no nível de risco associado ao sistema AAA, que é divido em:

> 1. riscos inaceitáveis: são considerados uma ameaça para pessoas como manipulação cognitivo-comportamental de pessoas;
> 2. riscos de alto risco: são os que representam risco de danos à saúde e segurança ou

> representar um risco de impacto adverso sobre os indivíduos e seus direitos fundamentais. Isto inclui sistemas AAA que são utilizados em produtos abrangidos pelo produto da UE legislação de segurança, como exemplos automóveis, aviação, dispositivos médicos, elevadores e brinquedos, com AAA;
> 3. risco limitado:como chatbots, IA generativa e sistemas AAA que geram ou manipulam imagens, áudio ou conteúdo de vídeo (ou seja, deepfakes). Esses sistemas terão que cumprir com requisitos de transparência, como divulgar que o conteúdo foi criado por IA.
> 4. risco mínimo: que representam risco baixo para os indivíduos como IA usada em jogos de computador e IA baseada filtros de spam. (English; Doherty; Stiernet, 2023, p. 3)

Assim, os sistemas AAA com risco insignificante para os humanos têm menos obrigações, enquanto aqueles que apresentam risco inaceitável são proibidos. Além disso, é obrigatória a realização de *Fundamental Rights Impact Assessment* (FRIA) - Avaliações de Impacto nos Direitos Fundamentais para todos os sistemas AAA de alto risco (English; Doherty; Stiernet, 2023).

Dessa forma, a Lei da Inteligência Artificial a ser aprovada pela União Europeia representa um marco histórico na regulamentação da IA adotando uma abordagem baseada no risco. Atualmente, encontra-se na fase final do processo legislativo, com as principais instituições da UE envolvidas nos trílogos para debater as disposições finais da lei.

Na etapa conclusiva das negociações, os modelos de fundação emergiram como ponto de discordância. Com a ascensão do ChatGPT, um chatbot popular baseado no potente modelo GPT-4 da OpenAI, os decisores políticos da UE estão ponderando sobre a melhor maneira de abordar esse tipo de IA na próxima legislação.

No último trílogo político, houve indícios de consenso para a introdução de normas específicas para os modelos de fundação, seguindo uma abordagem escalonada. A justificativa incluiu a preocupação de que a abordagem escalonada equivaleria a uma regulação no ordenamento e poderia comprometer a inovação e a abordagem baseada no risco. Isso implica a implementação de regras mais rigorosas para os modelos mais poderosos, destinados a ter um impacto mais significativo na sociedade (Bertuzzi, 2023).

Esta abordagem, alinhada com a Lei dos Mercados Digitais (DMA) e a Lei dos Serviços Digitais (DSA), foi percebida como uma concessão do Parlamento Europeu, que inicialmente preferia regras horizontais para todos os modelos fundamentais (Bertuzzi, 2023). Nesse sentido, Michele Loi (2023) analisa criticamente a implementação e o impacto da DSA da União Europeia, focando particularmente nas maneiras como as plataformas digitais de grande porte podem representar riscos sistêmicos à democracia através de suas operações e do uso de sistemas algorítmicos. A DSA foi criada para que plataformas muito grandes online identifiquem e mitiguem riscos sistêmicos decorrentes de seus design e funcionamento (Loi,

2023).

A estratégia escalonada tinha como objetivo impor obrigações mais rigorosas aos principais fornecedores, em sua maioria empresas não europeias. No entanto, grandes países europeus têm expressado uma crescente oposição a essa abordagem. Representantes de vários estados-membros, como França, Alemanha e Itália, manifestaram oposição a qualquer regulamentação para modelos de fundação (Bertuzzi, 2023).

Assim, propostas legislativas recentes na UE para abordar a responsabilidade por danos relacionados a IA, ainda necessitam ser consolidadas para efetivamente abordar os desafios trazidos pelos sistemas inteligentes. De modo geral, percebe-se que a Lei da IA na UE ressalta a importância do gerenciamento de riscos, que está vinculado a obrigações de *accountability* dos sistemas de IA. Isso inclui a exigência de preparar documentação técnica que detalhe as características gerais, capacidades e limitações dos sistemas, além de implementar medidas de transparência e estabelecer rotinas e procedimentos internos para garantir a governança de dados. Tais medidas enfatizam o papel duplo da responsabilidade civil, tanto em sua função promocional quanto precaucional.

Como debatido por Novelli *et al* (2024) no artigo "*Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity"*, as implicações legais e regulatórias da Inteligência Artificial Generativa, particularmente os Modelos de Linguagem de Grande Escala (LLMs), como o ChatGPT, no contexto da União Europeia tratam da atualização da Diretiva de Responsabilidade por Produtos Defeituosos (PLD).

Esta proposta estende o escopo da PLD para incluir todos os sistemas de IA e bens habilitados por IA, exceto softwares de código aberto. Essa extensão é significativa porque a PLD é o único regime de responsabilidade harmonizado na UE, aplicando uma responsabilidade estrita em certas circunstâncias (Novelli, *et al*.,2024).

Além disso, uma revisão geral da abordagem aos modelos de base exigiria uma profunda revisão da arquitetura de governança do regulamento e das disposições de responsabilidade ao longo da cadeia de valor da IA. Quando a Lei da IA foi proposta em abril de 2021, a UE estava na vanguarda da regulação global da Inteligência Artificial. No entanto, o aumento do interesse na IA por parte dos EUA, Reino Unido e China tem desafiado essa posição (Bertuzzi, 2023).

Vale lembrar que, enquanto a UE focalizou a supervisão da IA na privacidade, vigilância de dados e no potencial impacto sobre os direitos humanos, o Reino Unido examinou os chamados riscos existenciais associados aos modelos altamente capazes de uso geral, conhecidos por "IA de fronteira" (Sandle; Coulter, 2023).

Neste aspecto, cabe mencionar que os riscos específicos de segurança surgem na "fronteira" da IA referindo-se aos modelos de uso geral em grau elevado de qualificação, incluindo modelos básicos, que têm a capacidade de executar uma ampla variedade de tarefas. Além disso, há a consideração de IA estreita específica, relevante para situações em que podem surgir capacidades causadoras de danos, correspondendo ou ultrapassando as habilidades presentes nos modelos mais avançados atualmente. Riscos substanciais podem decorrer do uso intencional inadequado ou de problemas de controle não intencionais relacionados ao alinhamento com a intenção humana. Estas preocupações são devidas ao fato de que essas capacidades não são completamente compreendidas, tornando-as difíceis de prever (Sandle; Coulter, 2023).

Pode-se assim dizer que, a normativa da UE sobre o gerenciamento de riscos na área de robôs e IA destaca-se pela busca de um equilíbrio entre a promoção da inovação e a mitigação de riscos, por meio da integração gradual de princípios éticos e da cooperação internacional. Essa abordagem reflete o compromisso da UE em liderar a revolução tecnológica de maneira ética e responsável. No entanto, a falta de orientação específica da Comissão Europeia sobre como realizar avaliações de risco, torna incerto o processo de conformidade com os requisitos da DSA, perspectiva corroborada por Loi (2023).

4.3 ESTUDO COMPARADO ENTRE O GERENCIAMENTO DE RISCOS DA IA ENTRE AS NORMATIVAS DOS EUA E DO PARLAMENTO EUROPEU

Para uma análise aprofundada e coesa sobre o gerenciamento de riscos associados à inteligência artificial, especialmente em aplicações críticas como a cirurgia robótica, é essencial adotar uma abordagem estratégica. Esta abordagem inclui a identificação e avaliação de riscos específicos, a implementação de medidas de mitigação, e a adaptação contínua às mudanças tecnológicas e regulatórias. Em muitos casos, a prevenção e a gestão eficaz de riscos podem desempenhar um papel fundamental na proteção da sociedade.

As estratégias adotadas pela União Europeia (UE) e pelos Estados Unidos (EUA) para o gerenciamento de riscos de IA compartilham um conceito alinhado, reconhecendo os princípios de uma IA confiável e a importância de padrões internacionais. No entanto, ao se debruçar sobre as especificidades dos regimes de gerenciamento de risco, torna-se claro que há mais diferenças do que semelhanças entre eles. Particularmente em aplicações de IA ligadas a processos socioeconômicos e plataformas *online*, a UE e os EUA estão seguindo caminhos que refletem um desalinhamento significativo (Rosenvald, 2023).

Em 2017, nos Estados Unidos, ocorreu uma conferência significativa em Asilomar, Califórnia, com o propósito de estabelecer diretrizes para o avanço dos programas de inteligência artificial (Future of life Institute, 2017). Dessa conferência emergiram 23 princípios, que não apenas refletem o espírito do GDPR mas também propõem diretrizes axiológicas particulares para o campo. Foi enfatizado que os investimentos em inteligência artificial devem ser acompanhados por apoio financeiro para pesquisas que promovam sua aplicação benéfica e que deve existir uma interação produtiva entre os pesquisadores e os formuladores de políticas, visando cultivar uma cultura de cooperação, confiança e transparência. Esta iniciativa representa mais um esforço para desenvolver uma inteligência artificial que respeite os direitos fundamentais e a justiça social (Silva, 2021).

Na Conferência de Asilomar, ficou acordado que sistemas autônomos devem ser projetados para alinhar seus objetivos e comportamentos com os valores humanos, beneficiando o maior número possível de pessoas. No entanto, essa abordagem apresenta desafios, pois nem sempre é possível prever todas as atividades da IA, tornando o controle pelos desenvolvedores mais complexo. A conferência também consagrou o princípio do benefício compartilhado, que determina que as tecnologias de IA devem beneficiar o maior número de pessoas possível, incorporando uma ética utilitarista. No entanto, essa abordagem pode acarretar riscos aos valores fundamentais da pessoa humana sob um prisma individual.

Outra preocupação levantada foi que os sistemas de IA devem aprimorar, e não subverter, os processos sociais e cívicos essenciais para a saúde da sociedade. Além disso, a conferência concluiu que deve ser evitada uma corrida armamentista em armas autônomas letais, destacando a necessidade de esforços proporcionais de planejamento e mitigação para equilibrar o desenvolvimento da IA com a observância dos direitos fundamentais e do equilíbrio social.

Em termos legislativos, a cidade de Nova Iorque aprovou a Lei nº 1.696-A/2017, que busca garantir a transparência dos algoritmos utilizados pela administração pública. Essa lei define sistemas de decisão automatizada como implementações computadorizadas de algoritmos, incluindo aqueles derivados de aprendizado de máquina ou outras técnicas de processamento de dados ou inteligência artificial, usados para ajudar na tomada de decisões. Esta iniciativa reflete a tendência de legitimar a utilização de algoritmos em diversos setores sociais e assegura a responsabilidade civil em casos de equívocos ou falhas.

Adicionalmente, nos Estados Unidos, há discussões em andamento sobre a revisão da responsabilidade subjetiva, propondo regras adicionais que estabeleceriam um padrão de cuidado pré-determinado para os desenvolvedores e operadores de sistemas de IA. Essas

regras poderiam também facilitar a demonstração de presunção de culpa em casos de descumprimento. Se os critérios estabelecidos fossem cumpridos, caberia aos reclamantes provar a negligência real do desenvolvedor (Silva, 2021).

Por sua vez, a União Europeia tem buscado regulamentações robustas que, enquanto reconhecem a importância da inovação, procuram garantir a proteção de direitos e valores fundamentais. A diretiva europeia propõe uma abordagem legislativa mais ampla, impondo requisitos para aplicações de IA de alto risco em vários setores e promovendo a transparência em plataformas online e comércio eletrônico (Rosenvald, 2023).

Por outro lado, os EUA enfatizam a inovação, incluindo avaliações de *software*, como exemplo de reconhecimento facial, e amplo financiamento de pesquisa em IA, bem como na liberdade empresarial. Assim, adotam uma abordagem mais flexível e adaptável à regulação. O gerenciamento de riscos nos EUA é caracterizado por um esforço descentralizado, com várias agências federais adaptando-se de forma independente à IA (Rosenvald, 2023).

Ambas as abordagens destacam a importância de uma IA confiável e padrões internacionais, mas diferem significativamente em sua implementação e ênfase regulatória. A UE foca mais em regulamentações específicas para IA de alto risco, enquanto os EUA favorecem uma governança mais abrangente que exige ações específicas das empresas de tecnologia.

A gestão eficaz dos riscos associados ao desenvolvimento da IA é um desafio global que requer cooperação internacional, dada a sua natureza transfronteiriça. As abordagens divergentes dos EUA e da UE oferecem *insights* valiosos para o equilíbrio entre inovação e segurança. O desenvolvimento futuro de políticas deve considerar essas diferenças, visando criar um ambiente onde a IA possa prosperar de maneira responsável e segura.

A necessidade de uma abordagem determinante e estratégica é ainda mais evidente no contexto da cirurgia robótica. Nesse sentido, a Resolução do Parlamento Europeu de 16 de fevereiro de 2017, como já mencionado anteriormente, enfatiza a necessidade de categorizar robôs autônomos inteligentes com base em critérios como aquisição de autonomia através de sensores e interconectividade, autoaprendizado a partir de experiências e interações, um suporte físico mínimo, adaptação ao ambiente e a clara distinção de que eles não possuem vida no sentido biológico do termo.

Tal resolução ainda recomenda a adoção de sistemas como a "caixa-preta" para robôs cirúrgicos, o que é consistente com as discussões sobre *accountability* e explicabilidade em IA. Esses sistemas de registro oferecem um meio para documentar com precisão todas as operações e decisões tomadas pelo robô, o que torna imprescindível para investigar e entender

as causas de incidentes adversos.

Os eventos prejudiciais relacionados à cirurgia robótica, como os recalls do robô Da Vinci nos Estados Unidos, destacam os riscos associados a essas tecnologias avançadas. Entre 2000 e 2013, foram registrados significativos eventos adversos envolvendo o robô Da Vinci, incluindo casos de morte, lesões ao paciente e mau funcionamento do dispositivo. Esses incidentes sublinham a importância de considerar cuidadosamente os riscos ao avançar com tecnologias disruptivas na área da saúde (Nogaroli, 2023).

Nos EUA, a responsabilidade civil por danos decorrentes de cirurgias robóticas está fortemente baseada no sistema de direito comum (*common law*), que se apoia em precedentes judiciais e decisões de tribunais. A responsabilidade por produtos (*product liability*) é uma área bem estabelecida, e as empresas que fabricam robôs cirúrgicos podem ser responsabilizadas sob diversas teorias, incluindo negligência, responsabilidade estrita e quebra de garantia. Além disso, os Estados Unidos possuem um sistema de litígios altamente desenvolvido. Dessa maneira, a discussão legal em torno da responsabilidade em cirurgias robóticas também é um tema onde alguns argumentam que o sistema jurídico dos EUA é suficientemente flexível para acomodar novas tecnologias, como os robôs cirúrgicos Da Vinci (Hubbard, 2014).

Por outro lado, na União Europeia, a responsabilidade civil é regida principalmente pelo direito civil (*civil law*), com códigos e estatutos detalhados. A Diretiva sobre a Responsabilidade por Produtos Defeituosos (85/374/EEC) estabelece um regime de responsabilidade estrita para produtos defeituosos, incluindo dispositivos médicos e robôs cirúrgicos. Sob essa diretiva, os fabricantes podem ser responsabilizados por danos causados por um defeito no produto, independentemente de culpa. Além disso, a regulamentação e a harmonização das normas de responsabilidade civil entre os Estados-membros da UE fornecem um quadro mais uniforme em comparação com os EUA.

Quanto a abordagem regulatória, nos EUA, a Food and Drug Administration (FDA) regula dispositivos médicos, incluindo robôs cirúrgicos. O processo de aprovação pode ser rigoroso, mas uma vez aprovado, a responsabilidade por falhas muitas vezes recai sobre os fabricantes em caso de defeitos de design ou fabricação. Além disso, os hospitais e profissionais médicos podem enfrentar litígios por negligência médica, dependendo das circunstâncias do caso. Já na UE, a regulamentação de dispositivos médicos é gerida por uma combinação de regulamentos da UE e legislações nacionais. O Regulamento de Dispositivos Médicos (EU) 2017/745 (MDR) estabeleceu requisitos mais rigorosos para a aprovação e monitoramento pós-mercado de dispositivos médicos, incluindo robôs cirúrgicos. A

abordagem regulatória na UE tende a ser mais centralizada e harmonizada entre os Estados-membros, proporcionando um quadro regulatório mais consistente.

Portanto, em um contexto internacional mais amplo, pode-se observar que a Europa tem sido mais proativa e firme em suas recomendações e regulamentações sobre a inteligência artificial, embora muitas dessas normas sejam consideradas *soft laws*, como as Diretrizes Éticas para a Inteligência Artificial Confiável. Tais diretrizes, apesar de não coercitivas, são fundamentais para orientar a conduta ética no desenvolvimento dessa tecnologia. A Europa também possui uma legislação unificada que regula o tratamento de dados em todos os Estados-membros da União Europeia, consolidada no GDPR.

Em conclusão, enquanto a UE e os EUA compartilham princípios comuns sobre a IA confiável, suas estratégias de gerenciamento de riscos divergem, refletindo diferentes prioridades e abordagens regulatórias. A evolução da cirurgia robótica e os desafios legais associados reforçam a necessidade de uma abordagem cuidadosa e ponderada para mitigar os riscos, garantindo ao mesmo tempo o avanço tecnológico e a proteção da sociedade.

5 OS PARÂMETROS ATUAIS DA RESPONSABILIDADE CIVIL NA UTILIZAÇÃO DA IA NO CONTEXTO BRASILEIRO

Neste capítulo, propõe-se consolidar as análises realizadas com o objetivo de formular uma visão conclusiva sobre a capacidade do ordenamento jurídico brasileiro de enfrentar os desafios impostos pelo alargamento do protagonismo da IA e responder se o fabricante responde civilmente pelo risco do desenvolvimento. É fundamental destacar como as normas da Constituição Federal, do Código Civil (artigos 12; 186 e 187; e 927) e do Código de Defesa do Consumidor (artigos 12 e seguintes), combinado a leis especiais como a Lei Geral de Proteção de Dados e o Marco Civil da Internet (artigo 19), abordam a responsabilidade civil no contexto dos sistemas inteligentes autônomos. Além disso, os projetos de lei nº 2.630/2020, que trata da Liberdade, Responsabilidade e Transparência na Internet, e nº 2.338/2023 (artigos 27 a 29), que regula o uso da inteligência artificial, focando especialmente na IA e nos robôs cirurgiões dentro do quadro legislativo pertinente.

Inicialmente, discutimos a conceituação da inteligência artificial, um marco da era tecnológica que se destaca em diversos campos e facilita significativamente a vida humana. Em comparação com a operação manual tradicional, a IA apresenta uma autonomia e comportamentos independentes notavelmente superiores, capazes de operar sem intervenção humana e com potencial de aprendizado contínuo. Além de ser mais econômica e eficiente na prestação de serviços, a IA é frequentemente utilizada para substituir o trabalho humano. No entanto, sua implementação não está isenta de riscos e pode, a qualquer momento, resultar em violações de direitos, como acidentes médicos associados ao uso de produtos de IA no setor da saúde ou problemas relacionados a cirurgias robóticas.

Diante desses casos de infração, surge a necessidade de definir claramente como a responsabilidade por danos deve ser perpetrada e como o sistema legal pode ser aprimorado para abordar esses desafios. O desenvolvimento contínuo da indústria de inteligência artificial certamente acarretará uma série de problemas jurídicos e éticos que exigirão o suporte de um sistema legal robusto para sua resolução. Este capítulo visa, portanto, aprofundar a análise dessas questões, proporcionando um entendimento claro e direcionado sobre as implicações legais associadas ao avanço tecnológico.

5.1 A LEGISLAÇÃO BRASILEIRA SOB O OLHAR DOS RISCOS DA INTELIGÊNCIA ARTIFICIAL

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018 (Brasil, 2018), estabelece um marco fundamental na regulamentação do tratamento de dados pessoais no Brasil, incluindo dados relacionados à saúde. No seu artigo 6º, a lei delineia diversos princípios fundamentais para o tratamento adequado dos dados. Estes princípios incluem: i) a finalidade, que determina que o uso dos dados deve ter um propósito específico e claro; ii) a adequação, que assegura que os dados coletados sejam compatíveis com essa finalidade; iii) a necessidade, que restringe a coleta ao mínimo necessário para atingir os objetivos; iv) o livre acesso, que permite aos indivíduos acessar e verificar suas informações pessoais; v) a qualidade dos dados, exigindo que sejam precisos e atualizados; vi) a transparência, que requer clareza nas práticas de tratamento de dados; vii) a segurança, que envolve a implementação de medidas protetivas contra acessos não autorizados; viii) a não discriminação, que proíbe o uso discriminatório dos dados; ix) e a responsabilização e prestação de contas, que impõem aos agentes de tratamento a obrigação de demonstrar conformidade com esses princípios de forma proativa e documentada. Estes princípios visam a garantir que o tratamento de dados pessoais seja conduzido de forma ética e segura, protegendo os direitos fundamentais dos indivíduos.

Além desses princípios, o artigo 6º também menciona explicitamente: i) a licitude, que exige que o tratamento dos dados seja realizado de maneira legal e ética; ii) a lealdade, que implica um tratamento justo e honesto dos dados; iii) a limitação da conservação, que estabelece que os dados devem ser mantidos apenas pelo tempo necessário; iv) a integridade, que assegura que os dados sejam completos e não adulterados; e a v) confidencialidade, que protege os dados contra divulgação indevida.

No contexto do direito à saúde, a LGPD não apenas salvaguarda a privacidade e a integridade dos dados dos pacientes, mas também estabelece um quadro legal que assegura a confidencialidade necessária na relação entre profissionais de saúde e pacientes (Nogaroli, 2021). Essa legislação reconhece os dados de saúde como "dados sensíveis", sujeitos a proteções especiais e responsabilização, exigindo consentimento explícito do titular para seu uso e compartilhamento, exceto em casos previstos por lei ou para a proteção da vida e da saúde do titular.

Dessa forma, a implementação eficaz da LGPD no setor saúde implica em desafios e oportunidades, incluindo a necessidade de adaptação por parte de hospitais, clínicas e profissionais de saúde, que devem rever seus sistemas de gestão de dados para garantir conformidade legal e fortalecer a confiança dos pacientes. Este enquadramento legal não apenas protege indivíduos contra o uso indevido de seus dados, mas também promove uma

maior transparência na gestão de informações de saúde, essencial para a promoção de um atendimento ao paciente mais seguro e eficaz.

Vale lembrar também que a Lei nº 12.965, de 23 de abril de 2014 (Brasil, 2014), formalmente conhecida como o Marco Civil da Internet, estabelece princípios, garantias, direitos e deveres para o uso da internet no país. Em relação à responsabilidade civil, a legislação tem disposições específicas que tratam da responsabilidade dos provedores de aplicações de internet e dos provedores de conexão, como exemplo o disposto no art. 19 (Brasil, 2014).

O novo Projeto de Lei nº 2.338/2023 (Brasil, 2023), conhecido como o Marco Legal da Inteligência Artificial, está sendo discutido no Senado Federal e mescla outros projetos sobre o tema que tramitam na casa, como o PL 21/2020. O PL nº 2.338/2023, em seu art. 4º, inciso I, descreve um "sistema de inteligência artificial" como uma

> [...] máquina que opera com variados níveis de autonomia para atingir metas explícitas ou implícitas, e que deduz, com base em um conjunto de dados ou informações fornecidas, como produzir resultados, particularmente previsões, recomendações ou decisões que possam afetar ambientes virtuais ou reais. (Brasil, 2023).

Além disso, o texto categoriza diferentes tipos dessa tecnologia, incluindo a inteligência artificial generativa e a de propósito geral (SIAPG).

O marco legal da IA propõe uma metodologia de regulação da inteligência artificial baseada na classificação dos riscos associados e mostra similitudes tanto com o AI Act europeu quanto com o *AI Executive Order* dos Estados Unidos, adotando uma perspectiva híbrida que engloba várias áreas do governo. Esta proposta oferece respostas variadas para a responsabilidade civil, dependendo do nível de risco envolvido, seguindo exemplos de discussões similares que ocorrem na Europa e Estados Unidos. Sob as condições estipuladas pelo art. 27, § 1º do projeto (Brasil, 2023), os operadores ou fornecedores de sistemas de IA considerados de alto risco serão objetivamente responsáveis pelos danos causados, proporcionalmente à sua contribuição para o dano.

Dessa forma, semelhante à regulamentação da Europa, a proposta em discussão estipula uma avaliação preliminar de riscos antes que qualquer sistema de IA seja lançado no mercado. Sistemas considerados de risco excessivo serão proibidos, enquanto aqueles classificados como de alto risco serão regulados pela SIA (Sistema Nacional de Regulação e Governança de Inteligência Artificial). Para estes últimos, as empresas devem nomear um representante responsável pelo contato com as autoridades governamentais, encarregado de discutir aspectos como testes de confiabilidade e gestão de dados para evitar e prevenir vieses

discriminatórios, além de garantir a supervisão humana do sistema (Unzelte, 2024).

Estabelece ainda a proposta a obrigatoriedade de uma avaliação de impacto algorítmico em situações específicas. Adicionalmente, além da SIA, as empresas poderão formar associações privadas para autorregulação e definir seus próprios critérios técnicos. De acordo com Laura Schertel, a última versão da proposta trouxe avanços ao introduzir maior especificidade na classificação de riscos e maior flexibilidade para que agências setoriais incluam exceções (Mendes, 2024). Por outro lado, Rony Vainzof critica o projeto por apresentar uma "estrutura de governança extremamente densa, complexa e custosa" (Unzelte, 2024, p. 4).

Importante destacar que o PL nº 2.338/2023 (Brasil, 2023) estabelece claramente em seu artigo 29 que as responsabilidades civis resultantes de prejuízos provocados por sistemas de IA em contextos de relação de consumo devem seguir as normativas da Lei nº 8.078/1990. Portanto, a responsabilidade individual do médico, na qualidade de profissional liberal com relação ao paciente, continua sendo determinada com base na existência de culpa, conforme especificado no artigo 14, parágrafo 4º do CDC (Brasil, 1990).

Ainda no contexto brasileiro, o Projeto de Lei nº 2.630/2020, conhecido como Lei das Fake News (Brasil, 2020), traz seu foco principal em regular a disseminação de desinformação nas plataformas digitais e garantir maior transparência e responsabilização por parte das empresas que gerenciam essas plataformas. Embora tal projeto não aborde diretamente a questão da responsabilização de sistemas de IA em si, o debate que ele gera sobre tecnologia, privacidade, e ética pode influenciar futuras legislações que abordem mais diretamente a IA, especialmente em relação a como os sistemas de IA devem ser projetados, monitorados e regulados para evitar danos ou abusos. Assim, as discussões e regulamentações que ele propõe podem, eventualmente, influenciar como a responsabilidade por sistemas de IA será tratada.

Ao abordar as novas exigências das sociedades modernas e altamente tecnológicas, torna-se essencial discutir os princípios de uma ética responsável, que deve incluir compromissos futuros focados na prevenção e precaução. Neste contexto, a *accountability* em sistemas de inteligência artificial IA aplicados à saúde tem sido um tema amplamente debatido no Brasil. Um exemplo significativo é a Lei 14.510/2022, conhecida como Lei da Telessaúde, que enfatiza a necessidade de uma governança eficaz dos dados de saúde.

Os artigos 26-D e 26-E incorporados pela Lei da Telessaúde instituem a obrigação de cumprimento às normas expedidas pelo órgão de direção do Sistema Único de Saúde e às normas morais e éticas implementadas pelo Conselho Federal de Medicina. Além disso, por

tratar-se de atendimento médico prestado por meio virtual, a Lei da Telessaúde elencou, entre seus princípios, o da confidencialidade dos dados e o da responsabilidade digital (art. 26-A, IX). Esta legislação destaca a importância de adotar práticas e estratégias que assegurem o uso seguro e eficiente dos recursos telemáticos.

Merecem destaque os Protocolos Clínicos de Diretrizes Terapêuticas (PCDT) e as Diretrizes Diagnósticas e Terapêuticas (DDT), emitidos e atualizados pelo Ministério da Saúde, com o objetivo de orientar e padronizar o atendimento, diagnóstico e tratamento no âmbito do Sistema Único de Saúde (SUS). Em caso de alegação de erro médico, é necessário, antes de tudo, averiguar se o profissional cumpriu ou deixou de cumprir o Protocolo Clínico indicado para o caso concreto, cuja resposta será determinante para fixar sua responsabilidade civil, administrativa e até mesmo criminal (Santos, 2023)

Além disso, o conceito de responsabilidade digital foi introduzido como um princípio fundamental da telessaúde no artigo 2º da Lei nº 14.510/2022 (art. 26-A, IX, da Lei 8.080/90, lei do SUS). A responsabilidade digital, ou *accountability* digital, entende-se às obrigações de cuidado necessárias tanto em relação às ações (postar, curtir, comentar e compartilhar) quanto no que se refere ao fluxo de dados e informações no espaço digital da Internet. Dessa forma, a responsabilidade digital está ligada ao exercício da cidadania digital, onde os usuários são incentivados a usar a tecnologia de forma apropriada, consciente e não criminosa. Assim, tal responsabilidade ainda pode ser percebida como uma extensão da responsabilidade social colocada em prática no uso e gestão das tecnologias da informação e comunicação (TICs) (Santos, 2023).

Fernanda Schaefer relaciona este princípio ao conceito de *accountability*, que é um componente crucial da governança de dados. Isso não apenas reforça os padrões de responsabilidade civil, mas também estende sua aplicação para incluir medidas regulatórias preventivas. O objetivo dessas iniciativas é expandir o alcance da responsabilidade, integrando normas regulatórias que possam atuar tanto de forma preventiva (*ex ante*) quanto reativa (*ex post*), sempre com um foco na governança de dados (Schaefer, 2023).

Mais especificamente em relação à cirurgia robótica, a Resolução nº 2.311/2022 do CFM (CFM, 2022), que normatiza as cirurgias robóticas no Brasil, exemplifica claramente a responsabilidade de hospitais e clínicas médicas na adoção de tecnologias inovadoras. Conforme estabelecido no artigo 2º, essas instituições devem possuir as condições técnicas adequadas, incluindo equipamentos e instalações físicas apropriadas, além de serviços de suporte para lidar com qualquer intercorrência e recursos humanos capacitados para oferecer assistência especializada, conforme detalhado no Anexo 1 da Resolução. Adicionalmente, o

diretor técnico do hospital é responsável por verificar a documentação que comprova a capacitação e competência da equipe médica em lidar com a tecnologia, de acordo com o artigo 5º. Importante ressaltar também que a resolução estipula, nos artigos 3º e 4º e no Anexo 2, os requisitos específicos para a formação e treinamento dos médicos que utilizam essa tecnologia (CFM, 2022).

Dessa maneira, as instituições de saúde e os profissionais envolvidos devem assegurar que toda a tecnologia empregada esteja em perfeito estado de funcionamento e que as manutenções sejam realizadas regularmente, conforme as especificações do fabricante e as diretrizes da resolução, dada a complexidade e a precisão exigida em cirurgias robóticas. Uma vez não cumpridos tais requisitos, as entidades hospitalares podem responder objetivamente (Nogaroli, 2023).

Ademais, a responsabilidade civil pode ser implicada se um procedimento falhar devido à inadequação da formação recebida pelos médicos ou pela equipe técnica. Segundo a referida Resolução, é imperativo que todos os profissionais envolvidos passem por treinamentos específicos e mantenham suas certificações atualizadas para operar tais equipamentos (CFM, 2022).

Ainda na linha da Resolução nº 2.311/2022/CFM, é fundamental que os pacientes recebam todas as informações necessárias sobre os riscos, benefícios e alternativas às cirurgias robóticas. A responsabilidade civil pode ser envolvida se o consentimento informado não for adequadamente obtido, documentado ou se os pacientes não forem completamente esclarecidos sobre a natureza da tecnologia utilizada.

Nesse sentido, também se estende a responsabilidade civil à supervisão contínua e avaliação dos resultados das cirurgias robóticas. Hospitais e clínicas devem implementar protocolos para revisar e avaliar regularmente a eficácia e segurança dos procedimentos realizados com auxílio de robôs por meio de um programa de *compliance*[7] em conformidade com as diretrizes do comitê de bioética do nosocômio (Nogaroli, 2023). Isso inclui a notificação de quaisquer incidentes ou complicações que possam servir como base para revisão de práticas e possível responsabilização.

Após toda a análise e pesquisa realizada, acreditamos que aqui no Brasil ainda não temos uma legislação específica para tratar da responsabilidade civil por danos causados por cirurgiões robóticos. Em que pese a legislação brasileira atual tangenciar alguns pontos a

[7] Sobre o programa de *compliance*, Nogaroli discorre que, além de estar alinhado ao trabalho do comitê de bioética do hospital, deve cumprir pelo menos 5 (cinco) obrigações. Vide NOGAROLI, Rafaella. **Responsabilidade civil médica e inteligência artificial**: culpa médica e deveres de conduta no século XXI. São Paulo: Thomson Reuters. Brasil, 2023, p. 257.

temática, esta ainda está sendo aprofundada no projeto de novo código civil.

5.2 RESPONSABILIDADE CIVIL E IA CORRENTES DOUTRINÁRIAS

No presente tópico, exploramos a evolução e as nuances da responsabilidade civil dentro das sociedades tradicionais e modernas, destacando como o princípio da causalidade desempenha um papel central. De acordo com Rosenvald e Braga Netto (2024), a responsabilidade por danos é condicionada à comprovação de uma relação direta de causa e efeito entre a conduta do agente e o dano resultante. Esse conceito de responsabilidade civil pode variar significativamente, sendo interpretado em termos de compensação, punição ou prevenção, dependendo das particularidades temporais e geográficas.

Conforme estipulado pelo artigo 927 do Código Civil brasileiro, qualquer pessoa que, através de um ato ilícito (definidos nos artigos 186 e 187), cause dano a outrem é obrigada a repará-lo (Brasil, 2002). Essa norma enfoca a consequência do ato ilícito, não a conduta em si, alinhando-se com o conceito de responsabilidade civil extracontratual ou aquiliana, onde a sanção visa neutralizar os efeitos do dano e restaurar a ordem, na ótica detalhada por Rosenvald e Braga Netto (2024).

Assim, percebe-se que aquela norma se baseia na causalidade entre a ação e o dano resultante, enfatizando que a liberdade de ação de uma pessoa é limitada pela necessidade de não causar prejuízo a outrem. Este conceito de responsabilidade civil extracontratual, não visa punir a conduta em si, mas sim mitigar os efeitos de um dano causado, através da compensação.

A flexibilidade da responsabilidade civil, segundo apontam Gama e Viola (2021), permite sua adaptação às transformações jurídicas previstas na Constituição Federal. Dessa forma, integra-se de maneira eficaz ao Direito das Obrigações. Este ramo do direito impõe obrigações àqueles que violam deveres legais ou contratuais, realçando a complexidade e as adaptabilidades necessárias para lidar com as dinâmicas modernas das relações civis (Gama; Viola, 2021).

Maria Helena Diniz (2015, p. 34) complementa essa visão, ao descrever que:

> [...] a responsabilidade civil envolve medidas que obrigam a reparação de danos morais ou patrimoniais causados a terceiros, seja por ato próprio, de pessoa sob sua responsabilidade, ou de fato decorrente de coisas ou animais sob sua guarda. Isto engloba tanto a responsabilidade subjetiva, baseada na culpa, quanto a objetiva, imposta legalmente.

Historicamente, a responsabilidade civil evoluiu do direito romano e sua base na

vingança privada para um sistema mais civilizado focado na reparação dos danos. Savatier (1951) observa que essa transformação foi revolucionária, ampliando o dever de reparar danos causados por ações próprias ou por dependentes do agente. Lima (1998) argumenta que o aumento de vítimas das atividades humanas intensas levou à adoção da teoria da responsabilidade objetiva, focada na reparação independentemente da culpa, consolidada tanto na doutrina quanto no direito positivo.

Essa abordagem é reforçada pela teoria do risco, que introduziu a ideia de responsabilidade sem culpa, atribuindo a obrigação de reparar danos simplesmente pelo fato de uma atividade potencialmente perigosa ter causado um prejuízo. Isso reflete um movimento dentro do direito civil que prioriza a proteção dos interesses jurídicos sobre a punição da conduta, alinhando-se aos princípios constitucionais que enfatizam a prevenção de danos e a promoção da dignidade humana.

Avaliando a responsabilidade civil à luz dos princípios constitucionais, torna-se evidente que a legislação atual muda o foco do materialismo para a proteção dos direitos existenciais. A dignidade humana é princípio-chave na Constituição Federal e serve como alicerce ético. Assim, a promoção da pessoa como princípio constitucional se entrelaça com a responsabilidade civil, influenciando a forma como as leis são interpretadas e aplicadas. Isso orienta os julgadores a aplicar técnicas processuais que valorizam mais a prevenção do que a simples reparação dos danos, entrando em conformidade com uma abordagem mais humanista e proativa no tratamento da responsabilidade civil na sociedade contemporânea.

A respeito do princípio da prevenção, vale lembrar que a ideia de que é melhor prevenir danos do que reparar, tanto a medicina quanto a bioética adotam o princípio de *primum non nocere*, que significa “primeiro, não causar mal”. Esse princípio orienta a evitar causar prejuízos ao paciente acima de tudo. Por outro lado, o direito oferece proteção por meio de uma medida judicial preventiva que busca evitar atos ilícitos antes mesmo que qualquer dano ocorra, conforme estabelecido no artigo 497, parágrafo único, do Código de Processo Civil (Brasil, 2015).

A responsabilidade civil enfrenta, na sociedade automatizada e digital, complexidades crescentes devido às interações entre humanos e sistemas inteligentes. Esta nova realidade demanda uma reavaliação dos conceitos tradicionais de responsabilidade civil, especialmente com a possibilidade de proliferação dos danos causados por inteligências artificiais. No âmbito jurídico, surgem debates sobre a adequação dos institutos tradicionais para enfrentar os desafios impostos pelas transformações digitais.

Legisladores estão desafiados a desenvolver normas e padrões de responsabilidade que

acompanhem o rápido desenvolvimento tecnológico, buscando equilibrar inovação com as necessárias proteções aos usuários. A definição de padrões de responsabilidade apropriados é essencial para assegurar a confiança pública, promover a qualidade da inteligência artificial e da robótica, e garantir uma coexistência eficaz da tecnologia e seres humanos.

A responsabilidade civil relacionada à IA pode ser categorizada em dois tipos de regimes: objetivo e subjetivo. O regime objetivo é observado na responsabilização por defeitos do produto, e o subjetivo na responsabilidade por culpa. Isso inclui casos de produtos defeituosos ou falhas de programação, bem como situações de uso negligente ou imprudente da IA. Após pesquisas metodológicas realizadas, pode-se observar que a doutrina se divide em algumas correntes para explicar a responsabilização por danos decorrentes de IA, como veremos a seguir.

Uma das correntes de pensamento discute a dificuldade de atribuir responsabilidade civil à IA devido à sua natureza não humana e à opacidade dos processos decisórios em concordância com Xueting (2022). Esta corrente defende que penalizar os desenvolvedores por danos causados pela IA poderia inibir o avanço tecnológico. A teoria do risco do desenvolvimento, nesse contexto, é vista como uma possível excludente de responsabilidade, argumentando que a adoção da melhor tecnologia disponível no momento não deveria ser considerada um defeito da IA.

Contrapondo essa visão, há propostas para a criação de uma nova categoria jurídica, na linha da doutrina de Mafalda Barbosa, as "e-persons", que atribuiriam personalidade jurídica própria e patrimônio distinto aos sistemas de IA. Essa ideia, no entanto, encontrou resistência, pois a última Resolução do Parlamento Europeu, datada de 20 de outubro de 2020, sob o número 2020/2014(INL), descartou a possibilidade de atribuir personalidade jurídica aos sistemas operados por inteligência artificial, refletindo a complexidade e a controvérsia em estabelecer uma normativa consensual para essa nova realidade.

De modo geral, percebe-se que atribuir personalidade jurídica a robôs apresenta vários desafios. Primeiramente, conforme o relatório da Comissão Mundial para Ética do Conhecimento Científico e Tecnológico (COMEST) sobre ética em robótica da UNESCO (2017), é contraintuitivo considerar robôs como "pessoas" quando eles não manifestam características humanas fundamentais como vontade própria, intencionalidade, autoconsciência, capacidade moral e identidade pessoal, como mencionado no parágrafo 201. Em segundo lugar, a ideia de conceder personalidade jurídica aos robôs, apesar de se basear no conceito de pessoa jurídica e não em pessoas físicas, é problemática, pois, tradicionalmente, existe normalmente uma pessoa física responsável por trás de uma pessoa

jurídica, o que não se aplica a robôs autônomos. Além disso, o Comitê Econômico e Social Europeu, em sua sessão de 31 de maio de 2017, argumentou que comparar a responsabilidade limitada de empresas com robôs autônomos é inadequado porque, em última instância, potencialmente há uma pessoa física responsável nas corporações (Parágrafo 3.33). Por fim, mesmo que a finalidade de conferir personalidade jurídica a robôs seja criar um regime legal específico, como um *trust*, isso poderia inadvertidamente diminuir a responsabilidade do fabricante em caso de danos causados pela máquina (O´Sullivan; *et al*., 2019).

Outra corrente defende a responsabilidade subjetiva do programador, vinculando-a ao contrato de prestação de serviços. Por exemplo, se um sistema de IA for utilizado de forma inadequada, ou se as informações de treinamento do sistema forem insuficientes ou imprecisas, o proprietário/fornecedor ou operador do sistema pode ser considerado responsável pelos danos causados. Essa abordagem coloca o ônus da prova de culpa sobre a vítima, o que se torna desafiador dado o alto grau de autonomia da IA, que pode obscurecer o nexo causal entre a ação do programador e o dano ocorrido, como corroborado por Cerka, *et al.*, 2019.

Confirmando essa temática, Barbosa (2019) argumenta que a responsabilidade extracontratual baseada na culpa muitas vezes se mostra insuficiente. Em muitos casos, a culpa é evidente, como na falta de atualizações de *software* ou quebra de deveres de cuidado que permitam interferências externas, como ataques de *hackers*. No entanto, em outros casos, os danos podem ocorrer devido ao funcionamento autônomo normal da IA, desafiando as presunções tradicionais de culpa.

Nesse sentido, podemos levantar uma questão importante sobre a aplicabilidade do conceito de culpa em sistemas dotados de inteligência artificial, qual seja o regime de responsabilidade civil subjetivo pode ser insuficiente devido à complexidade probatória de demonstrar o nexo causal, semelhante ao que ocorreu durante o processo de industrialização, conforme também entendido por Queiroz (2020).

Para o usuário comum de sistemas de IA, pode ser quase impossível produzir evidências de culpa do responsável, seja o desenvolvedor do sistema ou o fabricante do produto, quando o comportamento do robô diverge de sua programação inicial de maneiras que podem levar a resultados prejudiciais. A imprevisibilidade, uma característica de sistemas que podem aprender e adaptar-se, coloca em questão se a responsabilidade deve recair sobre o fabricante, o programador, ou até mesmo o robô em si (Metz, 2016). Trata-se de uma complexidade adicional, onde a determinação da culpa pode variar conforme o caso específico. Portanto, em situações envolvendo danos causados por essas tecnologias, várias

partes podem ser responsabilizadas simultaneamente, como apoiado no entendimento de Mulholland (2019). Isso destaca a necessidade de repensar os paradigmas de responsabilidade civil para garantir uma distribuição justa de ônus e proteção.

Por sua vez, uma abordagem baseada na responsabilidade objetiva considera a IA como risco, ou um bem perigoso, aplicando a teoria do risco criado. Essa visão amplia a responsabilidade para aqueles que, mesmo sem agir de forma culposa, se beneficiam economicamente e poderiam mitigar os riscos associados à tecnologia. Nesse contexto, a responsabilidade não se restringe àqueles que agiram de forma culposa, mas recai sobre quem poderia minimizar riscos e lidar com impactos negativos. Introduz-se também a teoria do *deep-pocket*, a qual afirma que, em casos de danos causados por IA, a responsabilidade deve ser atribuída a entidades com capacidade financeira suficiente para compensar as vítimas, independentemente de sua culpa direta (Cerka *et al*., 2015). Dessa forma, a teoria do *deep-pocket* poderia reduzir o ônus sobre as vítimas que precisam provar o nexo causal em um setor tão técnico e opaco.

Importante estudo nas implicações da responsabilidade como explorado por O ´Sullivan *et al* (2018) deve estabelecer a classificação tripartida da responsabilidade: *accountability*, *liability* (responsabilidade legal) e *culpability* (culpabilidade). Essa estrutura serve como base para discutir como essas questões devem ser gerenciadas à medida que os robôs cirúrgicos se tornam mais autônomos. A discussão sobre a *accountability* de um robô cirúrgico é particularmente relevante, enfatizando a necessidade de sistemas de registro de dados que possam explicar e justificar decisões autônomas para garantir a segurança do paciente. Nesse sentido, a "*accountability* desses sistemas parece demandar, assim, um tipo de transparência *qualificada*. E, nesse cenário, o princípio da precaução, há muito invocado no campo da proteção ambiental, parece um *framework* útil para se pensar essa questão" (Bioni; Luciano, 2020, p. 3).

Adicionalmente, a corrente que advoga pela responsabilidade objetiva do fornecedor aplica o Código de Defesa do Consumidor, presumindo que qualquer dano causado por um defeito na IA, mesmo desconhecido no momento do desenvolvimento, deve ser indenizado. Esta abordagem reflete uma tentativa de harmonizar os princípios de proteção ao consumidor com os desafios trazidos pela tecnologia.

Quanto ao entendimento de produto defeituoso, observa-se que tal entendimento precisa ser aprimorado, devendo ser considerado defeituoso quando há uma falha em um dever geral de segurança, significando que desde sua colocação no mercado, já possuía tal defeito, como reforçado por Rosenvald; Braga Netto (2024). Além disso, o conceito de defeito

no produto também deve abranger aquele produto que não contem uma informação adequada e transparente. Em outras palavras, havendo um dever de informação, como visto no tópico específico, e esse dever não é satisfatoriamente cumprido, o produto torna-se defeituoso por vício de informação. Assim, a responsabilidade do fabricante não é excluída pela teoria do risco de desenvolvimento.

Discute-se também a possibilidade de atribuir responsabilidade a todos os envolvidos na cadeia de consumo por danos decorrentes de defeitos no produto ou serviço, estabelecendo a responsabilidade solidária entre desenvolvedores de *softwares*, fabricantes de produtos, e outros agentes na cadeia de fornecimento, conforme o artigo 7º, parágrafo único do Código de Defesa do Consumidor (Brasil, 1990). De maneira análoga ao estabelecido pelo Regulamento Geral sobre a Proteção de Dados (RGPD) da Europa, os incisos do § 1º do artigo 42 da LGPD estipulam claramente as situações em que operadores e controladores de dados serão solidariamente responsáveis.

Quando se discute inovação, frequentemente associa-se ao impacto nas relações de consumo. Isso ocorre porque, conforme destacado por Swanson em 2019, as legislações que regem a responsabilidade por danos ou defeitos em produtos continuam essenciais para salvaguardar os consumidores contra prejuízos, motivando as empresas a adotarem comportamentos responsáveis para minimizar riscos antecipáveis.

De modo geral, a responsabilidade objetiva de acordo com o CDC será aplicável ao fabricante de uma inteligência artificial autônoma quando um defeito no produto ou serviço for a causa direta de danos ao consumidor. Contudo, a maior complexidade desse cenário advém da dificuldade em provar o nexo de causalidade. Para tanto, em consonância com o pensamento de Henrique Sousa Antunes (2019), existe a necessidade de regimes jurídicos que empreguem modelos econômicos de causalidade para enfrentar os desafios impostos pela IA, sugere-se medidas como a inversão do ônus da prova e presunções de causalidade para facilitar a atribuição de responsabilidade em um cenário tão complexo.

A respeito da inversão do ônus probante, inspirada pelo RGPD europeu, o CDC também adotou a inversão do ônus da prova como uma exceção aplicável em três situações específicas: I) quando for verossímil a alegação; II) houver hipossuficiência para fins de produção de prova; ou III) quando a produção de prova pelo titular resultar-lhe excessivamente onerosa (Brasil,1990). Essa medida visa facilitar a defesa dos direitos dos consumidores em casos onde a obtenção de provas contrárias por parte do indivíduo seria excessivamente difícil.

Nessa linha, como ensina Faleiros Júnior é fundamental estabelecer claramente o nexo

causal, especialmente com um entendimento mais amplo dos riscos envolvidos. Isso leva à definição mais precisa de deveres (e consequentemente, mais passíveis de serem previstos), alinhando-se ao conceito de "previsibilidade", que se amolda à função preventiva no contexto atual da tecnologia (Faleiros Júnior, 2024).

A literatura internacional utiliza o termo *"foreseeability"* (previsibilidade), conforme explicado por Calo em 2015, para indicar que essa noção permanece essencial mesmo em casos de responsabilidade objetiva, onde não é necessário demonstrar negligência por parte do reclamante para obter reparação. Em situações onde sistemas emergentes interagem, pode ocorrer que tecnologias de outro modo úteis surpreendam todos os envolvidos (Calo, 2015). Se esses sistemas se mostrarem profundamente úteis para a sociedade, como muitos preveem, pode ser necessário desenvolver uma abordagem diferente da previsibilidade para avaliar responsabilidades. Assim, reconhece-se também a necessidade de expandir os critérios para melhor atender à função de precaução da responsabilidade civil (Faleiros Júnior, 2024). Com isso, amplia-se o conceito de responsabilidade civil para abarcar a *accountability*.

Para a disciplina jurídica da responsabilidade civil nos casos de inteligência artificial, é necessária uma abordagem sistemática, evitando tratamentos dispersos. Conforme entende O'Sullivan *et al*. (2019), a autonomia dos robôs cirúrgicos varia, e com ela varia o grau de responsabilidade e supervisão humana necessária. Em situações onde um robô cirúrgico opera sob controle direto humano, o cirurgião e o hospital normalmente retêm a responsabilidade legal pelos resultados da cirurgia. Nos casos de maior autonomia, onde o robô executa tarefas sem intervenção humana imediata, a responsabilidade pode se estender aos fabricantes dos robôs e aos desenvolvedores do *software*, especialmente se forem identificados defeitos de fabricação ou falhas de programação que levem a erros cirúrgicos.

Essa abordagem organizada e abrangente é essencial para adaptar a responsabilidade civil às novas realidades impostas pela tecnologia e as suas novas perspectivas, garantindo proteção adequada a todos os envolvidos. Atualmente no Brasil, o foco das discussões legislativas recai sobre o controverso Projeto de Lei nº 21 de 2020 (Brasil, 2020), que visa estabelecer bases, princípios e diretrizes para o desenvolvimento e implementação da inteligência artificial no país. Este projeto, que incorpora os Projetos de Lei números 5.051 de 2019 e 872 de 2021, tem sido objeto de amplas discussões pela Comissão de Juristas encarregada de fornecer apoio na elaboração de um substitutivo sobre a matéria, conhecida como CJSUBIA (Brasil, 2022).

A normatização da responsabilidade civil em relação à IA é, portanto, um campo de debate jurídico intenso e multifacetado. A busca por um equilíbrio entre proteção jurídica

adequada e incentivo ao avanço tecnológico requer uma abordagem normativa cuidadosa e adaptável às peculiaridades de cada caso. Na linha do sugerido por Tepedino e Silva (2019), é vital que os códigos civil e consumerista sejam aplicados nas relações de consumo, evitando a criação de um sistema normativo isolado para a IA, ou seja, um sistema de valores próprios da *lex robotica* (Ruffolo, 2017).

Com base na pesquisa sobre litígios relacionados a incidentes adversos na cirurgia robótica nos Estados Unidos, é evidente que a complexidade na análise da responsabilidade civil surge principalmente ao determinar a "causa eficiente do dano" e identificar quem deve ser responsabilizado pela compensação: fabricante, hospital ou médico, como corroborado por Kfouri Neto e Nogaroli (2020).

Fatos como Zarick *v.* Intuitive Surgical (2016) e Taylor v. Intuitive Surgical (2017), importantes no cenário jurídico norte-americano, foi debatida a responsabilidade civil do fabricante, seja por falta de divulgação adequada sobre indicações ou riscos relacionados ao uso do robô, seja por falhas no design de um instrumento robótico específico, que alegadamente teria resultado em queimaduras nos órgãos internos do paciente durante o procedimento cirúrgico (Kfouri Neto M, Nogaroli R., 2020).

Os avanços tecnológicos na área da saúde levantam importantes questões sobre o consentimento informado do paciente e a responsabilidade civil por eventos adversos durante procedimentos cirúrgicos assistidos por robôs. Em jurisprudências notáveis nos Estados Unidos, como a citada, a responsabilidade do fabricante foi discutida em relação à falta de informação sobre os riscos associados ao robô ou a defeitos em seu design, que supostamente causaram danos aos pacientes.

O estudo desses litígios revela a complexidade na análise da responsabilidade civil, especialmente ao determinar a causa eficiente do dano e quem deve ser responsabilizado: o fabricante, o hospital ou o médico. Por exemplo, se o médico não estiver diretamente vinculado ao hospital, mas apenas alugar espaço para realizar a cirurgia assistida por robô, o hospital não terá responsabilidade solidária pelas ações do profissional (Kfouri Neto M, Nogaroli R., 2020).

Outro ponto a considerar é o serviço paramédico, onde falhas na intervenção dos enfermeiros na configuração do robô ou na esterilização dos instrumentos robóticos podem levar a danos. Nos Estados Unidos, essas demandas são conhecidas como *"fingerpointing cases"*, pois há um dilema sobre quem deve ser responsabilizado em caso de danos ao paciente durante cirurgias robóticas: o médico (ou hospital) ou o fabricante do equipamento (Kfouri Neto M, Nogaroli R., 2020).

Segundo o Código de Defesa do Consumidor, há responsabilidade solidária na cadeia de fornecimento do produto, o que significa que o hospital pode ser responsabilizado pelos danos causados por defeitos no dispositivo médico, com direito a regresso contra o fabricante do robô. Isso significa que o hospital compartilha responsabilidade com o fabricante por falhas no dispositivo ou na informação fornecida ao paciente (Kfouri Neto M, Nogaroli R., 2020).

Vale lembrar que os riscos associados ao uso de robôs em cirurgias requer reflexão sobre como atribuir a responsabilidade civil entre os diversos agentes envolvidos, desde médicos e equipe de enfermagem até a entidade hospitalar e o fabricante do robô na linha do que também defende Kfouri Neto e Nogaroli (2020). Assim, mesmo com o implemento das inovações tecnológicas na área da saúde que potencialmente podem elevar os riscos de ocorrências danosas, como adverte Nogaroli (2023), é necessário averiguar a responsabilidade subjetiva do médico por "violação a um dever de conduta decorrente da boa-fé objetiva, tal como o dever de vigilância" (Nogaroli, 2023, p. 151).

Interessante ótica trazida por Anna Beckers e Gunther Teubner (2023), discute a adequação dos regimes de responsabilidade legal no contexto de algoritmos autônomos que atuam em instituições socio-digitais. Eles argumentam contra a aplicação de um regime uniforme de responsabilidade, favorecendo uma abordagem diferenciada que reconheça a diversidade dos contextos tecnológicos e sociais em que os algoritmos operam.

Beckers e Teubner utilizam uma tipologia de comportamento de máquinas, desenvolvida em estudos de TI, e teorias sociológicas e filosóficas para sugerir a base de três instituições sócio-legais emergentes: a personificação de atores não humanos, a associação humano-máquina como um sistema social emergente e a cognição distribuída na interconectividade de algoritmos. Os autores propõem regimes de responsabilidade que respondam adequadamente aos riscos associados a cada um desses contextos (Beckers; Teubner, 2023).

A discussão trazida por Beckers e Teubner é ilustrada com três casos hipotéticos: aconselhamento por robôs, os Panama Papers e o Flash Crash de 2010, mostrando como as lacunas de responsabilidade podem ser preenchidas de maneira mais eficaz por meio de uma diversificação dos regimes de responsabilidade legal. Eles argumentam que a responsabilidade não deve ser uniformemente aplicada, mas adaptada para refletir as nuances das interações entre algoritmos e a sociedade (Beckers; Teubner, 2023).

Beckers e Teubner (2023) sugerem que a lei de responsabilidade precisa assimilar elementos do direito público para responder à crescente digitalização do espaço público. Isso

inclui considerar os impactos dos algoritmos sobre os direitos fundamentais e a necessidade de adaptar as normas de responsabilidade para gerenciar os riscos associados à automação e à inteligência artificial. Beckers e Teubner apontam para a necessidade de uma "constituição digital" (*digital constitution*) que regule essas interações emergentes e os desafios apresentados pela tecnologia no espaço público (Beckers; Teubner, 2023, p. 99).

No caso de aconselhamento por robôs mencionado por Anna Beckers e Gunther Teubner, os autores examinam uma situação em que um tycoon de Hong Kong processou um corretor de investimentos por perdas significativas ocasionadas por decisões de um algoritmo autônomo. Este robô de aconselhamento, conhecido como K1, foi projetado para analisar sentimentos de investidores *online* e fazer previsões relacionadas ao futuro das ações dos EUA. Apesar de simulações promissoras inicialmente, o uso do robô em transações reais resultou em perdas substanciais (Beckers; Teubner, 2023).

A questão central levantada é o "problema da caixa preta": quando os humanos não conseguem entender as decisões do algoritmo, quem é responsável quando algo dá errado? A legislação atual não prevê compensação por danos se os atores humanos envolvidos cumprirem seus deveres de conduta, deixando uma lacuna significativa de responsabilidade. Por isso, a questão da "explicabilidade" e da *accountability* na IA deve ser prioritária, pois a capacidade de entender e explicar as decisões tomadas por sistemas autônomos é necessária para atribuir responsabilidade de forma justa e eficaz.

A integração desses conceitos desde as fases iniciais do desenvolvimento de IA pode facilitar a resolução de problemas legais que emergem com o uso dessas tecnologias avançadas, garantindo que os benefícios da IA sejam maximizados enquanto seus riscos são adequadamente gerenciados. Portanto, os engenheiros de IA devem considerar a "explicabilidade" como uma consideração primordial desde as fases iniciais do projeto. Assim, no próximo tópico será examinada a explicabilidade e a *accountability* a fim de buscarmos respostas para os problemas advindos dos sistemas inteligentes.

5.3 O DEVER DE INDENIZAR O DANO DECORRENTE DE UMA CIRURGIA ROBÓTICA E A EXPLICABILIDADE, ACCOUNTABILITY E COMPLIANCE

Na era da medicina avançada, a incorporação de robôs cirúrgicos equipados com inteligência artificial (IA) transformou significativamente as práticas médicas. Com essas inovações, emergem questões críticas de explicabilidade (explicação do processo decisório da IA) e *accountability*, particularmente em casos de incidentes adversos e a subsequente

obrigação de indenizar. A IA explicável (*explainable AI*), que surge do aprendizado de máquina (*machine learning*) com a inclusão de humanos na direção, é um desenvolvimento notável que aumenta a transparência das decisões autônomas e fortalece a confiança entre profissionais da saúde e pacientes (Shademan *et al*., 2016).

A explicabilidade da IA refere-se à capacidade de um sistema robótico justificar suas ações ou decisões de forma compreensível para humanos. Esta característica é necessária não apenas para a aceitação dessas tecnologias, mas também para a gestão de expectativas e a atribuição de responsabilidades quando os resultados cirúrgicos não são os esperados. Por exemplo, a compreensão dos fatores que levaram a uma decisão particular do robô torna-se importante em situações onde o resultado cirúrgico é negativo, a fim de se determinar a responsabilidade em tais cenários.

Para se entender melhor o conceito de explicabilidade, Herzog (2022) propõe fazer as perguntas: qual humano?, sob quais circunstâncias? e para quais propósitos? Segundo Floridi *et al*. (2020), a explicabilidade combina inteligibilidade (*intelligibility*) e *accountability*, permitindo que usuários e afetados compreendam e desafiem as interações e resultados dos sistemas de IA. A transparência é um componente essencial, exigindo a comunicação de todos os aspectos necessários para examinar ou desafiar um sistema robótico ao longo de seu ciclo de vida.

Contudo, a dificuldade em implementar a explicabilidade em sistemas complexos reside na natureza dos algoritmos de aprendizado profundo, que são intrinsecamente opacos e multicamadas, tornando desafiador identificar a contribuição exata de cada entrada para a decisão final. Esta complexidade impõe limitações significativas à capacidade de explicar e justificar as ações dos robôs cirúrgicos de forma que seja satisfatória e compreensível para os humanos envolvidos, em congruência ao pensamento de Shademan *et al*., 2016.

Além da explicabilidade, a responsabilidade em cirurgias robóticas envolve a adoção de medidas como sistemas de registro de "caixa-preta", que fornecem um registro detalhado das operações do robô, facilitando a análise de eventos adversos e ajudando na determinação da responsabilidade, como corroborado por Nogaroli, 2023. Nesse sentido, em termos práticos, a reparação por danos de um robô cirurgião frequentemente se resolve através do seguro, uma prática comum em medicina (Decker, 2014). Em outras palavras, a implementação de dispositivos de gravação, como caixas-pretas, foi proposta como uma forma de garantir a rastreabilidade das ações dos robôs e facilitar a atribuição de responsabilidade em caso de falhas ou danos (Palmerini *et al*., 2014).

Essa combinação de explicabilidade e *accountability* cria um arcabouço robusto para

estabelecer a culpa e o dever de indenizar danos resultantes de cirurgias robóticas. Em litígios, acessar e compreender as decisões da IA e as ações correspondentes do robô cirúrgico são fundamentais para estabelecer a responsabilidade. Em outras palavras, se, apesar das precauções realizadas pelo fornecedor, ocorrer o dano, a inobservância da *accountability* e explicabilidade é fator essencial para estabelecer o nexo de causalidade com vistas ao dever de indenizar.

Assim, destaca-se a importância da cooperação e da confiança (*trustworthy* AI) na criação de algoritmos, sublinhando a necessidade de sistemas colaborativos e uma cultura de responsabilidade e ética entre os profissionais, em coerência a Faleiros Júnior (2024). A aplicabilidade prática de conceitos como explicabilidade e *accountability* multicamadas apresenta desafios significativos, especialmente em sistemas de IA cuja complexidade pode tornar a transparência e a atribuição de responsabilidade em casos difíceis. Além disso, a constante evolução tecnológica pode superar rapidamente os marcos regulatórios existentes, exigindo uma adaptabilidade contínua das normas jurídicas.

A discussão sobre a responsabilidade legal e o dever de indenizar em cirurgias robóticas sublinha a urgência de desenvolver padrões e regulamentos que acompanhem o ritmo da inovação tecnológica. À medida que exploramos as fronteiras da medicina robótica, torna-se cada vez mais fundamental adotar práticas que promovam a transparência, a explicabilidade e a responsabilidade para proteger tanto pacientes quanto profissionais da saúde, assegurando que os benefícios dessas tecnologias sejam realizados de maneira ética e segura, consoante sopesado por Shademan *et al*., 2016.

Diante dos novos riscos e contingências introduzidos por tecnologias avançadas como robôs cirurgiões, a responsabilidade civil enfrenta desafios para lidar com os riscos associados a redes e sistemas inteligentes automatizados. O papel do *compliance* como mecanismo de gestão de riscos ganha destaque neste cenário, funcionando como uma estratégia para administrar os riscos de maior impacto negativo. O *compliance*, longe de se restringir a fórmulas prontas ou a uma interpretação rígida das normas, exige uma abordagem que considere a complexidade dos resultados das ações variadas.

Nesse sentido, como endossado por José Faleiros Júnior e Nelson Rosenvald, o *compliance* deve ser elevado à condição de valioso instrumento para identificar e quantificar responsabilidades, transcendendo sua função tradicional como mera ferramenta de conformidade regulatória e gestão de riscos.

Dessa forma, como estudado na presente dissertação, o dano ocasionado por um robô cirúrgico deve ser reparado de forma objetiva pelo fabricante do robô, ou seja,

independentemente de culpa. No entanto, se tal fabricante, ao produzir e colocar o produto no mercado, investiu em *compliance*, em outras palavras, adotou uma postura de conformidade com a lei e de adesão a parâmetros regulatórios, o valor do *quantum* da sua indenização pode ser reduzido.

O conceito de *accountability* é particularmente relevante para fabricantes e desenvolvedores de sistemas de cirurgia robótica, onde se espera o cumprimento rigoroso das normativas vigentes para mitigar riscos e garantir segurança. A legislação brasileira, em comparação com o direito comunitário europeu, opera sob uma presunção relativa de defeito do produto, facilitando o processo para o consumidor em casos de danos.

Essas iniciativas refletem uma preocupação crescente com os desafios que a responsabilidade civil enfrenta ao lidar com os riscos associados a sistemas inteligentes automatizados. As nuances dessas interações são essenciais para entender como a responsabilidade civil se adapta às complexidades introduzidas pelas novas tecnologias e as expectativas regulatórias, oferecendo uma visão aprofundada da aplicação da lei em contextos tecnologicamente avançados e altamente regulados.

Em linhas gerais, o estímulo constante à prevenção, princípio expresso da lei no art. 6º, VI, CDC (Brasil, 1990), incentiva a eliminação ou mitigação de danos e a propagação de uma cultura de boas práticas e de governança corporativa (Brasil, 1990). Ao analisar o regime de responsabilidade civil aplicável aos danos de sistemas inteligentes autônomos, como os robôs cirurgiões, a doutrina enfrenta o desafio de delimitar o risco previsto no art. 927, parágrafo único do Código Civil. A questão central já não é apenas estabelecer um nexo causal entre o dano e a conduta, mas entender se o dano ocorre dentro da esfera de risco da atividade. Se confirmado, pode haver um dever de indenizar, mesmo em contextos onde o nexo causal não é diretamente evidente.

Este exame reflete o desafio de abordar a responsabilidade civil com uma visão contemporânea, reconhecendo as peculiaridades trazidas pelas inovações tecnológicas e ajustando o quadro normativo para melhor atender às exigências da sociedade moderna. Ao fazer isso, a legislação não apenas protege os consumidores e usuários, mas também incentiva os desenvolvedores e fabricantes a manterem altos padrões de segurança e eficácia em suas operações e produtos.

É importante observar que, em muitos casos, os deveres que compõem a *accountability* e a *answerability* se articulam com a civil *liability*, seja no tocante à prevenção de danos, seja na configuração do nexo de causalidade para fins de determinação do dever de indenizar. Se entendermos a responsabilidade civil em seu sentido amplo e multifuncional, a

responsibility, a *accountability* e a *answerability* integram o sistema, funcionando como camadas capazes de dar respostas mais compreensivas ao fenômeno danoso, conforme corroborado por Rosenvald; Braga Netto (2024). Se tomarmos a responsabilidade civil em seu sentido clássico e estrito, com a função primordial de reparar o dano *a posteriori*, a *responsibility*, a *accountability* e a *answerability* ficam de fora do sistema, atuando ora como preceito ético informativo, ora em apoio à função reparatória, caso o dano se concretize (Santos, 2023).

Essas iniciativas refletem uma preocupação crescente com os desafios que a responsabilidade civil encara para lidar com os riscos associados a redes e sistemas inteligentes automatizados. A doutrina estrangeira aborda amplamente o conceito de *accountability*, principalmente porque este termo em inglês corresponde a um senso de responsabilidade. Autores como O'Sullivan *et al.* (2018) exploram o dever de indenizar pelos danos causados por cirurgiões robóticos sob esta ótica. Em contraste, no Brasil, o termo tem sido mais frequentemente associado à governança de dados, como estabelece a Lei Geral de Proteção de Dados Pessoais (LGPD). Dessa forma, sugere-se uma ampliação do instituto da responsabilidade civil para abranger novas perspectivas como a *liability, answerability, responsibility e accountability*.

5.4 ALGUNS DIRECIONAMENTOS DE COMO INDENIZAR

A responsabilidade civil dos fabricantes é objetiva, conforme entende a doutrina majoritária, mas o valor da indenização pode ser reduzido se houver evidências de que o fabricante investiu efetivamente em *compliance*, conforme o parágrafo único do art. 944 do Código Civil (Brasil, 2002). Este ponto é fundamental, pois destaca como as ações preventivas e a governança podem mitigar as responsabilidades legais.

Finalmente, exploramos o Código de Defesa do Consumidor (Brasil, 1990), enfatizando a proteção do paciente como consumidor de serviços médicos e a aplicabilidade da responsabilidade objetiva. Observa-se uma complexidade adicional introduzida pela legislação consumerista, particularmente os arts. 10 e 12 do Código de Defesa do Consumidor (CDC). O art. 12, § 1º do CDC detalha a definição de produto defeituoso como aquele que "não oferece a segurança que dele legitimamente se espera", considerando sua apresentação, os riscos razoáveis esperados e a época em que foi colocado em circulação (Brasil,1990).

Como também entende a autora Ana Elisabete Ferreira e Dias Pereira (2017), um produto é considerado defeituoso quando não oferece a segurança que se pode razoavelmente

esperar dele em todas as circunstâncias, incluindo como é apresentado, como pode ser utilizado e quando foi colocado no mercado. Adicionalmente, existe ilicitude quando ações ou omissões violam normas técnicas ou deveres básicos de precaução, resultando na violação de direitos ou interesses protegidos por lei. Danos causados por equipamentos ou produtos que apresentem falhas são também uma forma de ilicitude, assim como quando tais violações decorrem do funcionamento inadequado do serviço.

Em outras palavras, pode-se dizer que um produto é considerado defeituoso quando não atende às expectativas de segurança baseadas em seu uso, apresentação e data de lançamento. Além disso, ele expande a discussão para incluir a noção de ilicitude, detalhando que ocorre tanto por ações ou omissões que violam normas técnicas ou deveres de cuidado, de informação, quanto por danos resultantes de defeitos nos produtos ou falhas no serviço. No entanto, se o fabricante ou desenvolvedor dos sistemas inteligentes autônomos demonstrou a devida *accountability*, seu dever de indenizar pode ser atenuado.

Essas nuances são fundamentais para compreender como a responsabilidade civil se adapta às complexidades introduzidas pelas novas tecnologias e às expectativas regulatórias. O entendimento da presunção relativa do nexo causal e do defeito do produto, juntamente às observações sobre risco e responsabilidade civil, oferece uma visão aprofundada da aplicação da lei em contextos tecnologicamente avançados e altamente regulados.

Além disso, nos casos Zarick v. Intuitive Surgical (2016) e Taylor v. Intuitive Surgical (2017), importantes questões legais foram levantadas em relação à responsabilidade e segurança no uso de robôs cirúrgicos desenvolvidos pela Intuitive Surgical. Esses casos destacam os desafios e as implicações jurídicas que surgem quando a tecnologia avançada é integrada à prática médica, incluindo a adequação dos treinamentos fornecidos, a divulgação de riscos e a eficácia dos dispositivos durante as operações.

Estamos então apontando para o uso de produto ou serviço no modelo "*AI-as-tool*" ou "*Robot-as-toll*", ou seja, a responsabilidade por danos causados por atos autônomos dos médicos robôs devem recair sobre seus fornecedores ou seus desenvolvedores, já que os médicos robôs são reconhecidos pela legislação e jurisprudência simplesmente como ferramentas.

Em suma, este capítulo discutiu importantes direcionamentos sobre como pode ser estabelecida a indenização no âmbito da responsabilidade civil envolvendo produtos e serviços tecnológicos avançados, como é o caso dos sistemas autônomos usados em procedimentos médicos cirúrgicos. A legislação atual, embora robusta, como os códigos civilista e consumerista, além da LGPD, enfrenta desafios singulares ao tentar enquadrar

novas tecnologias sob o arcabouço legal existente. As discussões acerca da definição de produtos defeituosos, a aplicação da responsabilidade objetiva e a relevância de ações preventivas e de *compliance* são essenciais para entender como indenizações podem ser ajustadas ou mitigadas em face de incidentes envolvendo dispositivos médicos inteligentes.

Observou-se a complexidade das interações entre normas preexistentes e as adaptações necessárias para abarcar as especificidades dessas novas tecnologias, ressaltando a influência significativa das práticas de *compliance* e *accountability* na mitigação de riscos legais. A análise dos marcos legais e das posições doutrinárias revela um panorama dinâmico, onde a adequada compreensão da aplicabilidade da responsabilidade objetiva e das nuances de ilicitude assume um papel central. Ainda verifica-se que mesmo com a implementação de *accountability* e explicabilidade algorítmica, se o dano ocorrer, o descumprimento dessas normas é essencial para estabelecer o nexo de causalidade, fundamentando o dever de indenizar.

Para garantir a segurança e a ética no uso de sistemas inteligentes autônomos, é essencial desenvolver e implementar normas específicas que regulem a utilização de IAs, assegurando que todos os desenvolvedores, fabricantes e operadores cumpram padrões rigorosos de segurança. Além disso, é necessário criar agências reguladoras para supervisionar a experimentação e a implementação de novos modelos robóticos na área médica, garantindo que todos os testes sejam conduzidos de modo confiável e ético. Também é fundamental fornecer treinamento adequado a todos os profissionais que utilizam esses sistemas, assegurando que compreendam os riscos envolvidos e saibam como minimizar potenciais danos. Finalmente, deve-se garantir a transparência na comunicação dos riscos associados ao uso de tecnologias inteligentes, tanto para os profissionais da saúde quanto para os pacientes, permitindo uma tomada de decisão informada.

Tais *insights* reforçam a necessidade de mais estudos e de um debate contínuo para refinar as abordagens legais, garantindo tanto a segurança dos usuários quanto a justa responsabilização dos fornecedores e desenvolvedores dessas tecnologias. Portanto, este é apenas um entre vários panoramas possíveis, e a evolução da legislação e da jurisprudência será decisiva para definir os contornos futuros da justa atribuição de responsabilidades no contexto da medicina robótica e da inteligência artificial.

6 CONSIDERAÇÕES FINAIS

A revolução da cirurgia robótica tem sido uma das mais significativas inovações na medicina contemporânea, transformando radicalmente as abordagens cirúrgicas e prometendo uma nova era de procedimentos autônomos de alta precisão. A crescente integração da inteligência artificial na cirurgia robótica autônoma levanta importantes questões éticas, legais e de responsabilidade.

Nosso posicionamento destaca a necessidade de avanços técnicos para capturar as diferentes premissas da responsabilidade, tal como abarca a doutrina estrangeira no que se refere a *responsibility*, *accountability* e *answerability*, visando garantir a confiabilidade desses sistemas autônomos. O entendimento dos significados e das múltiplas expressões do termo responsabilidade na doutrina estrangeira, como as de língua inglesa, possivelmente servirá para compreender a estrutura e o funcionamento do sistema moderno de responsabilidade civil, principalmente em razão do avanço e uso dos sistemas inteligentes autônomos.

Nessa dissertação, delineia-se uma agenda de pesquisa abrangente para alcançar esse objetivo, o trabalho aborda a necessidade de representação e raciocínio sobre responsabilidade tanto prospectivamente (para tarefas futuras) quanto retrospectivamente (para falhas que já ocorreram). Isso permitirá uma melhor compreensão de quem pode ser considerado responsável em diferentes contextos. Destaca, ainda, o papel fundamental do raciocínio sobre responsabilidade em todas as etapas do *design*, desenvolvimento e implementação de sistemas autônomos confiáveis. O que inclui a consideração de responsabilidade em áreas como cirurgia robótica, onde erros podem ter consequências significativas para pacientes e profissionais de saúde.

Além disso, reconhece-se a importância de proteger os valores existentes dos direitos: Constitucional, Civil e do Consumidor, enquanto promovemos a inovação. Propõe-se um regime de responsabilidade objetiva para lesões pessoais e morte.

No contexto da cirurgia robótica autônoma, foi identificado desafios únicos relacionados à integração da IA e aprendizado de máquina (ML). Embora, esses sistemas ofereçam benefícios significativos, como precisão aprimorada e redução de erros humanos, também levantam questões éticas, legais e de segurança que exigem atenção cuidadosa.

Este trabalho buscou estabelecer um *roadmap* e agenda de pesquisa sobre como a noção de responsabilidade pode oferecer conceitos de solução inovadores para garantir a confiabilidade e legalidade dos sistemas autônomos por meio das novas premissas da responsabilidade civil. Por meio desse esforço, buscou-se promover uma integração eficaz das

tecnologias de IA na sociedade, mantendo o respeito pelos valores éticos e legais fundamentais.

Assim, nas considerações finais desta dissertação, refletimos sobre os principais achados relacionados à explicabilidade algorítmica e *accountability* em sistemas de IA, com um enfoque particular em robôs cirurgiões. Ao explorar a legislação e as regulamentações vigentes tanto nos Estados Unidos quanto na União Europeia, foi possível identificar como diferentes jurisdições estão moldando o desenvolvimento e a aplicação da IA de maneira a alinhar-se com os princípios éticos e legais de proteção dos direitos fundamentais, de dados e responsabilidade civil.

A análise do CDC e do CC no contexto brasileiro revelou como a responsabilidade civil é atribuída no caso de falhas, defeitos do produto, ou danos causados por sistemas autônomos, incluindo robôs cirúrgicos. Esses dispositivos, ao operarem dentro de um quadro legal que ainda está se adaptando às novas tecnologias, apresentam desafios particulares quanto à atribuição de culpa e determinação de responsabilidade.

A importância da explicabilidade nos sistemas de IA foi um ponto central, especialmente no que tange à capacidade de os sistemas serem transparentes e compreensíveis para os usuários, incluindo tanto os profissionais de saúde quanto os pacientes nos casos de cirurgia robótica. A necessidade de sistemas que não apenas executem suas funções eficazmente, mas que também possam explicar suas decisões de maneira inteligível, torna-se fundamental para a construção de confiança e para a aceitação social da tecnologia.

A *accountability*, ou responsabilização, foi outro tema importante discutido, sublinhando a necessidade de sistemas de IA que não só respeitem os regulamentos existentes, mas que também sejam capazes de demonstrar proativamente essa conformidade através de documentação e práticas recomendadas. Este aspecto é especialmente significativo quando consideramos o potencial de IA, como os robôs cirúrgicos, para afetar de forma profunda a vida e a saúde dos pacientes.

Pelas pesquisas realizadas, foi possível observar que, no contexto da IA autônoma, a teoria do risco do desenvolvimento não é uma excludente de responsabilidade por danos causados. Assim, os fabricantes e desenvolvedores dessas tecnologias podem ser responsabilizados mesmo se eles empregaram a tecnologia mais avançada disponível na época, e que, inicialmente, não apresenta defeitos evidentes, ao lançar o produto no mercado. Ainda, sugerimos a redução do *quantum* indenizatório na medida em que o agente tenha investido em *compliance* para evitar as consequências indesejadas e prestado a devida *accountability*. O *compliance* é destacado como um mecanismo de gestão de riscos, exigindo

uma abordagem que considere a complexidade dos resultados das ações. O *compliance* deve ser elevado à condição de instrumento para identificar e quantificar responsabilidades, transcendendo sua função tradicional.

A revolução da cirurgia robótica tem sido uma das mais significativas inovações na medicina contemporânea, transformando radicalmente as abordagens cirúrgicas e prometendo uma nova era de procedimentos autônomos de alta precisão. A crescente integração da inteligência artificial na cirurgia robótica autônoma levanta importantes questões éticas, legais e de responsabilidade.

Nosso posicionamento enfatiza a necessidade de avanços técnicos para capturar as diferentes premissas da responsabilidade, tal como abarca a doutrina estrangeira no âmbito da *responsibility*, *accountability* e *answerability*, visando a garantir a confiabilidade desses sistemas autônomos. Assim, destaca-se a necessidade de representação e raciocínio sobre responsabilidade, tanto prospectivamente (para tarefas futuras) quanto retrospectivamente (para falhas que já ocorreram), para uma melhor compreensão de quem pode ser considerado responsável em diferentes contextos.

Além disso, reconhecemos a importância de proteger os valores existentes dos direitos: Constitucional, Civil e do Consumidor, enquanto promovemos a inovação. Dessa maneira, se faz necessário uma proposta de um regime de responsabilidade objetiva para lesões pessoais.

Ao explorar as legislações e as regulamentações vigentes nos Estados Unidos e União Europeia, foi possível identificar como diferentes jurisdições estão moldando o desenvolvimento e a aplicação da IA. Essas normativas procuram alinhar-se com os princípios éticos e legais de proteção dos direitos fundamentais, de dados e a responsabilidade civil. Nos EUA, a responsabilidade civil por danos decorrentes de cirurgias robóticas baseia-se no sistema de *common law*, com um sistema de litígios altamente desenvolvido. As empresas podem ser responsabilizadas sob diversas teorias, como negligência e responsabilidade estrita. Por outro lado, na UE, a responsabilidade civil é regida pelo *civil law*, com a Diretiva sobre a Responsabilidade por Produtos Defeituosos estabelecendo um regime de responsabilidade estrita.

Diante dessas complexidades, torna-se cada vez mais claro que a medicina e, especialmente, os cirurgiões robôs constituem um campo fértil para o avanço do debate sobre ética e regulamentação. A cirurgia robótica, enquanto promete melhorar a precisão, reduzir tempos de recuperação e minimizar erros humanos, também coloca novos desafios que precisam ser endereçados através de estudos rigorosos e regulamentações apropriadas.

A integração de sistemas robóticos em procedimentos cirúrgicos não é apenas uma questão de melhoria técnica, mas também de reflexão profunda sobre como estruturamos a responsabilidade e a governança dessas tecnologias. Isso implica considerar cuidadosamente como tais tecnologias podem ser implementadas de maneira que respeitem os direitos dos pacientes e garantam um alto nível de segurança e eficácia.

A necessidade de novos estudos é evidente, pois estes ajudarão a moldar um ambiente onde a tecnologia não apenas coexista com princípios éticos fundamentais, mas também os promova, considerando todos os aspectos de responsabilidade e *accountability*. Estudos futuros deverão explorar não apenas os aspectos técnicos da cirurgia robótica, mas também as implicações sociais, éticas e legais dessa integração. Isso inclui a compreensão de como os sistemas de IA podem ser auditados e regulados de maneira eficiente e transparente, e como podem ser projetados para serem responsivos às necessidades e preocupações dos usuários finais – os pacientes.

Portanto, à medida que avançamos na era da automação em medicina, é imperativo que o desenvolvimento de políticas, a formação de consensos éticos e a pesquisa acadêmica avancem a par com as inovações tecnológicas. Só assim será possível garantir que o uso de cirurgiões robôs contribua efetivamente para a evolução da medicina, promovendo melhorias significativas na qualidade dos tratamentos e na segurança dos pacientes, enquanto abordamos de maneira eficaz e proativa os desafios éticos e legais impostos por tais tecnologias.

Na medicina avançada, a utilização de robôs cirúrgicos com inteligência artificial (IA) tem transformado as práticas médicas, levantando questões de explicabilidade e accountability, especialmente em casos de incidentes adversos e obrigações de indenizar. A IA explicável é crucial para aumentar a transparência das decisões autônomas e fortalecer a confiança entre profissionais de saúde e pacientes. A explicabilidade da IA refere-se à capacidade de um sistema robótico de justificar suas ações de forma compreensível para humanos, essencial para aceitar essas tecnologias e atribuir responsabilidades em casos de resultados cirúrgicos negativos.

Herzog (2022) sugere perguntas para entender a explicabilidade, enquanto Floridi et al. (2020) combinam inteligibilidade e accountability para que os usuários compreendam e desafiem as interações da IA. A transparência é fundamental, exigindo a comunicação de todos os aspectos necessários para examinar um sistema robótico. A complexidade dos algoritmos de aprendizado profundo torna desafiadora a explicação e justificação das ações dos robôs cirúrgicos.

A responsabilidade em cirurgias robóticas envolve medidas como sistemas de registro

de "caixa-preta", facilitando a análise de eventos adversos e a determinação da responsabilidade. A reparação por danos de um robô cirúrgico frequentemente se resolve através do seguro. A combinação de explicabilidade e accountability é essencial para estabelecer a culpa e o dever de indenizar em litígios.

A cooperação e a confiança são cruciais na criação de algoritmos, destacando a necessidade de sistemas colaborativos e uma cultura de responsabilidade e ética. A constante evolução tecnológica exige adaptabilidade contínua das normas jurídicas. A discussão sobre responsabilidade legal e dever de indenizar em cirurgias robóticas sublinha a urgência de desenvolver padrões e regulamentos que acompanhem o ritmo da inovação tecnológica.

O dano ocasionado por um robô cirúrgico deve ser reparado de forma objetiva pelo fabricante, mas o valor da indenização pode ser reduzido se o fabricante tiver adotado uma postura de conformidade com a lei.

A legislação brasileira opera sob uma presunção relativa de defeito do produto, facilitando o processo para o consumidor em casos de danos. Essas iniciativas refletem uma preocupação com os desafios que a responsabilidade civil enfrenta ao lidar com os riscos de sistemas inteligentes automatizados. A análise do regime de responsabilidade civil aplicável aos danos de sistemas inteligentes autônomos enfrenta o desafio de delimitar o risco previsto no art. 927, parágrafo único do Código Civil.

A responsabilidade civil deve ser entendida em seu sentido amplo e multifuncional, integrando *accountability* e *answerability* para dar respostas compreensivas ao fenômeno danoso. A doutrina estrangeira explora amplamente o conceito de *accountability*, enquanto no Brasil, o termo tem sido mais associado à governança de dados. Sugere-se uma ampliação da responsabilidade civil para abranger novas perspectivas como *liability, answerability, responsibility* e *accountability.*

Ao concluir, esta dissertação reforçamos a necessidade de um quadro regulatório robusto e adaptativo que possa acompanhar o ritmo acelerado da inovação tecnológica. A colaboração entre legisladores, desenvolvedores de tecnologia, profissionais jurídicos e a comunidade médica é essencial para garantir que a introdução de tecnologias avançadas como a IA em ambientes críticos, como o cirúrgico, seja realizada de forma responsável, ética e segura, maximizando benefícios e minimizando riscos.

Portanto, é evidente que, apesar da crescente adoção de tecnologias inovadoras no campo da saúde, a legislação brasileira ainda precisa evoluir para tratar de maneira mais específica e abrangente a responsabilidade civil em casos de danos causados por cirurgiões robóticos. Atualmente, a legislação brasileira não é satisfatoriamente capaz de atender aos

reclamos da responsabilidade civil por danos advindos de inteligência artificial. Por isso, é imperativa a necessidade de um aprofundamento da temática, como está sendo realizado no anteprojeto do Código Civil, para assegurar diretrizes claras e específicas que protejam os pacientes e responsabilizem adequadamente os profissionais e instituições de saúde envolvidos.

REFERÊNCIAS

AFFONSO, Filipe José Medon. **Inteligência Artificial e Danos:** autonomia, riscos e solidariedade. 2019. 268 f. Dissertação (Mestrado em Direito Civil) – Faculdade de Direito, Universidade do Estado do Rio de Janeiro, Rio de Janeiro.

ANTUNES, Henrique Sousa. Inteligência Artificial e responsabilidade civil: enquadramento. **Revista de Direito da Responsabilidade**. Coimbra, ano 1, 2019. Disponível em: https://revistadireitoresponsabilidade.pt/2019/inteligencia-artificial-e-responsabilidade-civil-enquadramento/. Acesso em: 22 jan. 2024.

ARENDT, Hannah. **A Condição Humana**. Tradução: Roberto Raposo, 10 ed., Rio de Janeiro: Forense Universitária, 2005, p. 48.

ASIMOV, Issac. **Eu, robô**. Tradução de Aline Storto Pereira. São Paulo: Aleph. 2014.

ASIMOV, Issac. **Los Robots y el imperio**. Tradução de Rosa N. de Naveira. Buenos Aires: Emecé Editores S.A. Edición digital, 2002. p. 239.

BALLEL, Teresa Rodríguez de Las Heras. La inteligencia artificial en clave jurídica: Propuesta de conceptualización y esbozo de los retos regulatorios. Una mirada Europea. In: ***Revista de Ciencia de la Legislación***, Buenos Aires, n. 8, outubro de 2020.

BARBOSA, Mafalda Miranda. **Inteligência Artificial, E-Persons e Direito: Desafios e Perspectivas**. Disponível em: http://www.cidp.pt/revistas/rjlb/2017/6/2017_06_1475_1503.pdf . Acesso em: 18 maio 2023.

BARBOSA, Mafalda Miranda. Inteligência artificial e blockchain: desafios para a responsabilidade civil. **Revista de Direito da Responsabilidade**. Ano 1, 2019, p. 2-3.

BARFIELD, Woodrow (Editor). **The Cambridge Handbook of the Law of Algorithms**. Cambridge: Cambridge University Press, 2021.

BECKERS, Anna; TEUBNER, Gunther. Responsability for algorithmic misconduct: unity or fragmentation of liability regimes?. **The Yale Information Society Project & Yale Journal of Law and Technology Digital Public Sphere Series**. 2023. Disponível em: https://law.yale.edu/isp/publications/digital-public-sphere/uniformity-and-fragmentation-digital-public-sphere/responsibility-algorithmic-misconduct-unity-or-fragmentation-liability-regimes Acesso em: 13 maio 2024.

BERTUZZI, Luca. EU's AI Act negotiations hit the brakes over foundation models. Euractiv.com, 25 out. 2023. **Euractiv**. Disponível em: https://www.euractiv.com/section/artificial-intelligence/news/eu-policymakers-enter-the-last-mile-for-artificial-intelligence-rulebook/. Acesso em: 05 abr. 2024.

BIONI, Bruno Ricardo; LUCIANO, Maria. **O princípio da precaução na regulação de inteligência artificial**: seriam as leis de proteção de dados o seu portal de entrada? Disponível em: https://brunobioni.com.br/wp-content/uploads/2019/09/Bioni-Luciano_O-PRINCI%C C %81PIO-DA-PRECAUC%CC%A7A%CC%83O-PARA-REGULAC%CC%A7A%CC% 83

O-DE-INTELIGE%CC%82NCIA-ARTIFICIAL-1.pdf. Acesso em: 23 abr. 2024.

BODIN DE MORAES, Maria Celina. LGPD: um novo regime de responsabilização civil dito proativo. **Civilistica.com**, Rio de Janeiro, v. 8, n. 3, p. 1–6, 2019. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/448. Acesso em: 07 mai. 2024.

BRAGA NETTO, Felipe Peixoto. Novo Manual de Responsabilidade Civil. 4ª ed., rev. São Paulo: Editora JusPodivm, 2024. 960 p.

CALIXTO, Marcelo Junqueira. **A Responsabilidade Civil do Fornecedor de Produtos pelos Riscos do Desenvolvimento.** Rio de Janeiro: Renovar, 2004.

CALIXTO, Marcelo Junqueira. O art. 931 do Código Civil de 2002 e os riscos do desenvolvimento. In **Revista Trimestral de Direito Civil**, vol. 20, Out/Dez. 2004, p. 53-94.

CALIXTO, Marcelo Junqueira; BILLWILLER, Stefannie. A Responsabilidade civil pelos danos causados por sistemas de inteligência artificial. **Editora Forum - Coluna Direito Civil.** 19 set. 2022. Disponível em: https://editoraforum.com.br/noticias/responsabilidade-civil-pelos-danos-causados-por-sistemas-de- inteligencia-artificial-coluna-direito-civil/ Acesso em: 9 nov 2023.

CALVO COSTA, Carlos A. El significado y las especies de daño resarcible. **Revista de Derecho de Daños.** 2012 v. 3. P. 193-227. Disponível em: http://ccalvocosta.com.ar/articulos/El%20significado%20y%20las%20especies%20de%20da%C3%B1o%20resarcible.pdf. Acesso em: 12 abr 2024.

CASTELLS, Manuel. **A Sociedade Em Rede**. Ed.Paz & Terra. 2013. p. 630.

CERKA, Paulius; GRIGIENE Jurgita; SIRBIKYTÈ, Gintarè. Liability for damages caused by artificial intelligence. **Computer Law & Security Review**, n. 31, 2015. p. 376-389.

CHAVES, Natália Cristina. **Inteligência artificial: os novos rumos da responsabilidade civil.** In: VII Encontro Internacional do CONPEDI Braga - Portugal, 2017. Disponível em: https://www.conpedi.org.br/publicacoes/pi88duoz/c3e18e5u/7M14BT72Q86shvFL.pdf. Acesso em: 22 maio 2023.

COMANDÉ, Giovanni. Intelligenza Artificiale e responsabilità tra liability e *accountability*: il carattere trasformativo dell'IA e il problema della responsabilità. In: NUZZO, Antonio; OLIVIERI, Gustavo (a cura di). **Analisi giuridica dell'Economia**. Studi e discussioni sul diritto dell'impresa. Bolonha: Il Mulino, 2019, v. 1. p. 169-188.

CORDEIRO, António Barreto Menezes. **Da responsabilidade civil pelo tratamento de dados pessoais**. In: BARBOSA, Mafalda Miranda; ROSENVALD, Nelson; MUNIZ, Francisco (coord.). Desafios da nova responsabilidade civil. Salvador: JusPODIVM, 2019. p. 49-64.

CORDEIRO, António Barreto Menezes. Repercussões do RGPD sobre a responsabilidade civil. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro. São Paulo: **Revista dos Tribunai**s, 2019. p. 777-795.

COZMAN, Fabio Gagliardi. No canal da Inteligência Artificial – Nova temporada de desgrenhados e empertigados. **Estudos Avançados** 35 (101), 2021. Disponível em: https://www.scielo.br/j/ea/a/q3MZJVGqtrrhrYWZy4vt54w/?format=pdf. Acesso em: 20 set 2023.

DASGUPTA P, Jones A, Gill IS. Robotic urological surgery: a perspective. **BJU International**. 2005 Jan; 95(1):20-23. DOI: 10.1111/j.1464-410x.2005.05241.x. PMID: 15638888. Disponível em: https://europepmc.org/article/MED/15638888 Acesso em: 10 fev. 2024.

DE TEFFÉ, C. S.; MEDON, F. Responsabilidade Civil e Regulação de Novas Tecnologias: Questões acerca da utilização de Inteligência Artificial na tomada de decisões empresariais. **REI - Revista Estudos Institucionais**, *[S. l.]*, v. 6, n. 1, p. 301–333, 2020. DOI: 10.21783/rei.v6i1.383. Disponível em: http://estudos.homologacao.emnuvens.com.br/REI/article/view/383. Acesso em: 28 set. 2023.

DIGNUM, Virgnia. **Responsible Artificial Inteligence**: How to Develop and Use AI in a Responsible Way. Springer Nature Switzerland, 2019. ISBN 978-3-030-30370-9 ISBN 978-3-030-30371-6. v. 22, p 133.

DRESCH, Rafael de Freitas Valle; FALEIROS JÚNIOR, José Luiz de Moura. **Reflexões sobre a responsabilidade civil na Lei geral de proteção de dados (Lei nº 13.709/2018)**. In: ROSENVALD, Nelson; DRESCH, Rafael de Freitas Valle; WESENDONCK, Tula (coord.). Responsabilidade civil: novos riscos. Indaiatuba: Foco, 2019. p. 65-89.

DONEDA, Danilo Cesar Maganhoto; MENDES, Laura Schertel; SOUZA, Carlos Affonso Pereira de; ANDRADE, Noberto Nuno Gomes de. Considerações iniciais sobre inteligência artificial, ética e autonomia pessoal. **Pensar: Revista de Ciências Jurídicas**, Fortaleza, v. 23, n. 4, p 1-17, out/dez.2018. Disponível em: https://www.researchgate.net/publication/330299671_Consideracoes_iniciais_sobre_inteligencia_ar tificial_etica_e_autonomia_pessoal. Acesso em: 20 maio 2023.

ENGLISH, Steve; DOHERTY, Ashlee; e STIERNET, Maud. Body of Knowledge (BoK): Fundamental Rights Impact Assessments (FRIA). August 2023. Disponível em: https://forhumanity.center/European Parliament Resolution of 16 February 2017 with Recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL). (2017). Acesso em: 30 nov. 2023.

EVANGELISTA, Rafael. (2018), "Review of Zuboff's 'The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power'. **Surveillance & Society** 17, 1/2: 246-251. Disponível em: https://doi.org/10.24908/ss.v17i1/2.13132. Acesso em: 17 set. 2023.

EZRACHI, Ariel; STUCKE, Maurice. **Artificial Intelligence & Collusion:** WhenComputers Inhibit Competition. University of Illinois Law Review, 10 mar. 2017. Disponível em: https://www.illinoislawreview.org/wp-content/uploads/2017/10/Ezrachi-Stucke.pdf. Aceso em: 17 set. 2023.

FALEIROS JÚNIOR, José Luiz de Moura. **A evolução da inteligência artificial em breve**

retrospectiva. In: BARBOSA, Mafalda Miranda *et al*. (coord.). Direito digital e inteligência artificial: diálogos entre Brasil e Europa. Indaiatuba: Editora Foco, 2021.

FALEIROS JÚNIOR, José Luiz de Moura. Responsabilidade por falhas de algoritmos de inteligência artificial: ainda distantes da singularidade tecnológica, precisamos de marcos regulatórios para o tema? **Revista de Direito da Responsabilidade**, Coimbra, v. 4, p. 906-933, 2022.

FALEIROS JÚNIOR, José Luiz de Moura. **Explicabilidade algorítmica e responsabilidade civil**. 2 abr. 2024 Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-responsabilidade-civil/404514/explicabilidade-algoritmica-e-responsabilidade-civil. Acesso em: 3 maio 2024.

FERREIRA, Jussara Suzi Assis Borges Nasser; ROSA, André Luís Cateli. Fornecimento eletrônico de dados pessoais dos consumidores: responsabilidade civil objetiva e solidária e o dano social. **Revista de Direito do Consumidor**, v. 28, n. 122, p. 233-266, mar./abr. 2019.

FERREIRA, Yuri. Robô teria queimado e rasgado mulher com câncer que morreu após cirurgia, diz processo. **Revista Fórum**. 2024. Disponível em: https://revistaforum.com.br/ciencia-e-tecnologia/2024/2/10/rob-teria-queimado-rasgado-mulher-com-cncer-que-morreu-apos-cirurgia-diz-processo-153799.html. Acesso em: 12 maio 2024.

FORNASIER, Mateus de Oliveira. Questões fundamentais acerca da responsabilidade civil da inteligência artificial. **Civilistica.com.** Rio de Janeiro, a. 11, n. 2, 2022. Disponível em: https://civilistica.com/questoes-fundamentais-acerca/. Acesso em: 07 maio 2023.

FRAZÃO, Ana. MULHOLLAND, Caitlin. **Inteligência artificial e Direito: Ética, Regulação e Responsabilidade**. São Paulo: Thomson Reuters Brasil, 2019. p. 85.

FRAZÃO, Ana. **Algoritmos e inteligência artificial**. Jota, publicado em 15 de maio de 2018. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/algoritmos-e-inteligencia-artificial-15052018. Acesso em: 08 set. 2023

FROOMKIN, A. M. (2016). **Introduction**: Robot Law. In Ryan Calo, A. Michael Froomkin & Ian Kerr, Robot Law. Northampton – MA: Edward Elgar, 2016.

FUTURE OF LIFE INSTITUTE. **Asilomar AI principles**. 11 ago. 2017. Disponível em: https://futureoflife.org/ai-principles/. Acesso em: 5 abr. 2024.

GAINES, James. Handing the Surgeon's Scalpel to a Robot. **Knowable Magazine**. 14 set. 2022. Disponível em: **https://www.medscape.com/viewarticle/980798? src=WNL_mdpls_220921_mscpedit_surg&uac=360794CK&spon=14&impID=4665999#vp_2.** Acesso em: 11 fev. 2024.

GAMA, Guilherme Calmon Nogueira da; VIOLA, Rafael. Perspectivas sobre o nexo de causalidade: passado, presente e futuro. **Revista de Direito Civil Contemporâneo**. v. 29. ano 8. p. 207-240. São Paulo: Ed. RT, out./dez. 2021. p. 208.

HART, H. L. A.; HONORÉ, Tony. **Causation in tort the law**. Second Edition. Oxford:

Clarendon Press, 1985, reprinted, 2002.

HERZOG, Christian. On the risk of confusing interpretability with explicability. **AI and Ethics**. 2022. V. 2. ed. 1. pág 219-225.

HUME, David. **Investigación sobre el conocimiento humano**. Trad. Jaime de Salas Ortueta. Madrid: Alianza, 1988, p. 87.

JAMJOOM AA, Jamjoom AM, Marcus HJ: Exploring public opinion about liability and responsibility in surgical robotics. **Nat Mach Intell.** 2020, 2:194-6. Disponível em: 10.1038/s42256-020-0169-2 Acesso em: 05 mai. 2024.

KFOURI NETO M, Nogaroli R. **Estudo comparatístico da responsabilidade civil do médico, hospital e fabricante na cirurgia assistida por robô**. In: Martins GM, Rosenvald N. Responsabilidade civil e novas tecnologias. Indaiatuba: Foco; 2020. p. 399-428.

KFOURI NETO M, Nogaroli R. **Responsabilidade civil pelo inadimplemento do dever de informação na cirurgia robótica e telecirurgia:** uma abordagem de direito comparado (Estados Unidos, União Europeia e Brasil). In: Rosenvald N, Menezes JB, Dadalto L. Responsabilidade Civil e Medicina. Indaiatuba: Foco; 2020. p. 159 -186.

LACERDA, Bruno Torquato Zampier. **Estatuto jurídico da Inteligência Artificial**: entre categorias e conceitos, a busca por marcos regulatórios. - lndaiatuba, SP: Editora Foco, 2022, p. 216.

LIMA, Alvino. **Culpa e risco**. 2. ed. rev. e atual pelo Prof. Ovídio Rocha Barros Sandoval. São Paulo: Editora Revista dos Tribunais, 1998. - (RT Clássicos) ISBN 85-203-1663-8.

LEITE, José Rubens Morato. **Dano ambiental**: do individual ao coletivo, extrapatrimonial. 2 ed. rev. e atual. e ampl. São Paulo: RT, 2003. p. 28.

LEHMANN, J., Breuker, J. & Brouwer, B. Causation in AI and Law. **Artif Intell Law** 12, 279–315. 2004. Disponível em: https://doi.org/10.1007/s10506-005-4157-y. Acesso em: 15 mar. 2024.

LOI, Michele. **How to define platforms' systemic risks to democracy**. 1 ago. 2023. Disponível em: https://algorithmwatch.org/en/making-sense-of-the-digital-services-act/. Acesso em: 12 fev. 2024.

MACHADO, Lécio Silva. Médico robô: responsabilidade civil por danos praticados por atos autônomos de sistemas informáticos dotados de inteligência artificial. **Lex Medicinae Revista Portuguesa de Direito da Saúde**. Ano 16 - n.º 31-32 – Jan./Dez. 2019.

MAKARY, M. A.; Daniel, M. Medical error-the third leading cause of death in the US. **BMJ Clinical research ed**., 2016, 353, i2139. Disponível em: https://doi.org/10.1136/bmj.i2139. Ou https://www.bmj.com/content/353/bmj.i2139 . Acesso em:17 mai. 2024.

MAGRANI, Eduardo; SILVA, Priscilla; VIOLA, Rafael. **Novas perspectivas sobre ética e responsabilidade de Inteligência Artificial**. In: FRAZÃO, Ana; MULHOLLAND, Caitlin (coords.). Inteligência Artificial e Direito: ética, regulação e responsabilidade. São Paulo:

Thomson Reuters Brasil, 2019.

MASCITTI, M. LA FUNCIÓN PREVENTIVA DE LOS DAÑOS CAUSADOS POR LA ROBÓTICA Y LOS SISTEMAS AUTÓNOMOS. **Revista Brasileira de Direitos Fundamentais & Justiça**, *[S. l.]*, v. 16, n. 1, p. 15–54, 2022. DOI: 10.30899/dfj.v16i1.1319. Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/1319. Acesso em: 1 fev. 2024.

MATTHIAS, Andreas. The responsibility gap: ascribing responsibility for the actions of learning automata. **Ethics and Information Technology**, v. 6, issue 3, set. 2004. Disponível em:https://onlinelibrary.wiley.com/doi/10.1002/rcs.1968. Acesso em: 11mai. 2024.

MEDON, Filipe. Inteligência Artificial e Responsabilidade Civil: Autonomia, Riscos e Solidariedade. Salvador: JusPodivm, 2019. p. 448.

MELO, Bricio Luis da Anunciação; CARDOSO, Henrique Ribeiro. Sistemas de inteligência artificial e responsabilidade civil: uma análise da proposta europeia acerca da atribuição de personalidade civil. **Direitos Fundamentais & Justiça**, Belo Horizonte, ano 16, p. 89-114, out. 2022.

MENCZER, F., CRANDALL, D., Ahn, YY. *et al.* **Addressing the harms of AI-generated inauthentic content**. *Nat Mach Intell* 5, 679–680 (2023). Disponível em: https://doi.org/10.1038/s42256-023- 00690-w. Acesso em: 02 fev. 2024.

MENDES, Gilmar Ferreira. **Curso de direito constitucional**. 10. ed. São Paulo: Saraiva, 2015.

MENEZES, Joyceane Bezerra de; COELHO, José Martônio Alves; BUGARIM, Maria Clara Cavalcante. A expansão da responsabilidade civil na sociedade de riscos. **Scientia Iuris**: Londrina, v. 15, n. 1, p. 29-50, jun. 2011.

MENDES, Laura Schertel. Autodeterminação informativa: a história de um conceito. **Pensar - Revista de ciências jurídicas**. 2020. Fortaleza. v. 25, n. 4, p. 1-18. e-ISSN:2317-2150. Disponível em: (https://periodicos.unifor.br/rpen/article/view/10828). Acesso em: 20 maio 2023.

MENDES, Laura Schertel. MATTIUZZO, Marcela. Discriminação Algorítmica: Conceito, Fundamento Legal e Tipologia. **Revista de Direito da Univille.** Porto Alegre, v. 16, n. 90, 2019, 39-64, nov-dez 2019.

MILARÉ, Édis. **Direito do ambiente**. 11. ed. São Paulo: Revista dos Tribunais, 2018.

MONTEIRO, Renato Leite. Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil? Artigo estratégico 39. Dezembro de 2018. In: MULHOLLAND, Caitlin. **Responsabilidade civil e processos decisórios autônomos em sistemas de inteligência artificial (IA): autonomia, imputabilidade e responsabilidade**. In: FRAZÃO, Ana. MULHOLLAND, Caitlin (coord.). Inteligência artificial e direito: ética, regulação e responsabilidade. Ed. Revista dos Tribunais. São Paulo: Brasil, 2019.

MORAES, Maria Celina Bodin de. LGPD: um novo regime de responsabilização dito ”proativo”.**Civilística**. A. 8, n. 3, 2019. Disponível em: http://civilistica.com/lgpd-um-

novo-regime-de-responsabilizacao-civil-ditoproativo/. Acesso em: 25 ago. 2023.

MOREIRA, Fernando. Paciente morre após erro de robô durante cirurgia cardíaca. Disponível em: https://extra.globo.com/noticias/page-not-found/paciente-morre-apos-erro-de-robo-durante-cirurgia-cardiaca-23216846.html Acesso em: 05 abr. 2024.

MORRELL, A. L. G. *et al*.. Evolução e história da cirurgia robótica: da ilusão à realidade. **Revista do Colégio Brasileiro de Cirurgiões**, v. 48, 2021. Disponível em: https://doi.org/10.1590/0100-6991e-20202798 ou em https://www.scielo.br/j/rcbc/a/4qVcw3NC75jwPNtkgkhwSWf/?lang=pt# . Acesso em: 23 mar. 2024.

MULHOLLAND, Caitlin Sampaio. **A responsabilidade civil por presunção de causalidade**. Rio de Janeiro: GZ Editora, 2010. p. 308.

MULHOLLAND, Caitlin Sampaio. **Responsabilidade civil e processos decisórios autônomos em sistemas de inteligência artificial (IA): autonomia, imputabilidade e responsabilidade**. In: FRAZÃO, Ana. MULHOLLAND, Caitlin (coord.). Inteligência artificial e direito: ética, regulação e responsabilidade. Ed. Revista dos Tribunais. São Paulo: Brasil, 2019.

NOGAROLI, Rafaella. Implicações ético jurídicas da medicina robótica e inteligência artificial nas cirurgias e cuidados na saúde. Disponível em: https://academiamedica.com.br/blog/implicacoes-etico-juridicas-da-medicina-robotica-e-inteligencia-artificial-nas-cirurgias-e-cuidados-da-saude#!#_edn32. Acesso em: 01 fev. 2024.

NOGAROLI, Rafaella e KFOURI NETO, Miguel. Procedimentos cirúrgicos assistidos pelo robô Da Vinci: benefícios, riscos e responsabilidade civil. **Cadernos Ibero-Americanos de Direito Sanitário**, *[S. l.]*, v. 9, n. 3, p. 200–209, 2020. Disponível em: https://www.cadernos.prodisa.fiocruz.br/index.php/cadernos/article/view/615. ou em DOI: 10.17566/ciads.v9i3.615. Acesso em: 2 fev. 2024.

NOGAROLI, Rafaella. **Responsabilidade civil médica e inteligência artificial**: culpa médica e deveres de conduta no século XXI. São Paulo: Thomson Reuters. Brasil, 2023. p. 337.

NORONHA, Fernando. **Desenvolvimentos contemporâneos da responsabilidade civil**. Seqüência: Estudos Jurídicos e Políticos, Florianópolis, p. 21-37, jan. 1998. ISSN 2177-7055. Disponível em: //antigo.periodicos.ufsc.br/index.php/sequencia/article/view/15533/14089. Acesso em: 19 ago 2023.

NORVIG, Peter; RUSSELL, Stuart J. **Artificial Intelligence:** A Modern Approach. New Jersey: Prentice Hall, 1995.

NOVELLI, Claudio and Casolari, Federico and Hacker, Philipp and Spedicato, Giorgio and Floridi, Luciano. **Generative AI in EU Law**: Liability, Privacy, Intellectual Property, and Cybersecurity (January 14, 2024). Available at SSRN: https://ssrn.com/abstract=4694565 or http://dx.doi.org/10.2139/ssrn.4694565.

O'SULLIVAN, S., NEVEJANS, *et al*. (2019). Legal, regulatory, and ethical frameworks for development of standards in artificial intelligence (AI) and autonomous robotic surgery. *The*

International Journal of Medical Robotics and Computer Assisted Surgery, *15*(1). Disponível em: https://doi.org/10.1002/rcs.1968 Acesso em: 03 fev. 2024.

PAGALLO U. **The Laws of Robots**—Crimes, Contracts, and Torts. Law, Governance and Technology Series 10, Springer 2013:I-XXV;1–200.

PALMERINI E *et al*. **Regulating emerging robotic technologies in europe**: robotics facing law and ethics. In: D6.2 Guidelines on Regulating Robotics; 2014. Disponível em: http://www.robolaw.eu/. Acesso em 11 mai. 2024.

PARLAMENTO EUROPEU. Resolução do Parlamento Europeu, de 16 de fevereiro de 2017, que contém recomendações à Comissão sobre disposições de Direito Civil sobre Robótica (2015/2103(INL). Disponível em: http://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_PT.html. Acesso em: 20 jan. 2024.

PARLAMENTO EUROPEU. Resolução do Parlamento Europeu, de 20 de outubro de 2020, que contém recomendações à Comissão sobre um regime de responsabilidade civil para a inteligência artificial. Bruxelas: Parlamento Europeu, 2020. Disponível em: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0277_PT.html. Acesso em: 15 set. 2023.

PASQUALE, Frank. Oxford Handbook of Ethics of AI. 2021.

PASQUALE, Frank. **When Medical robots fail**: Malpractice principles for an era of automation. Disponível em: PASQUALE, Frank. Oxford Handbook of Ethics of AI. 2021. Acesso em: 3 mai. 2024.

PEREIRA, Uiara Vendrame; TEIXEIRA, Tarcisio. Inteligência artificial: a quem atribuir responsabilidade? **Revista Direitos Garantias Fundamentais.** Vitória, v. 20, n. 2, p. 119-142, maio/agosto, 2019.

PIRES, Thatiane Cristina Fontão; SILVA, Rafael Peteffi da. A responsabilidade civil pelos atos autônomos da inteligência artificial: notas iniciais sobre a resolução do Parlamento Europeu. **Revista Brasileira de Políticas Públicas**, v. 7, n. 3, p. 238-254, 2017. Disponível em: DOI: 10.5102/rbpp.v7i3.4951. Acesso em: 15 abr. 2023.

PIRES, Thatiane Cristina Fontão. **Desenvolvimento e aplicação da compensatio lucri cum damno no direito alemão**: O problema da cumulação da indenização com vantagens advindas do evento danoso/Thatiane Cristina Fontão PIRES; orientador, Rafael Peteffi da SILVA, 2019. 254 p. Dissertação (mestrado) - Universidade Federal de Santa Catarina, Centro de Ciências Jurídicas, Programa de Pós-Graduação em Direito, Florianópolis, 2019.

PORTO, Uly de Carvalho Rocha. **A responsabilidade civil extracontratual por danos causados por robôs autônomos.** 2018. Dissertação (Mestrado em Ciências Jurídico-Civilistas), Faculdade de Direito da Universidade de Coimbra, Coimbra, 128 p.

QUINELATO DE QUEIROZ, João. **Responsabilidade civil no uso de inteligência artificial**: imputação, culpa e risco. In: TEPEDINO, Gustavo; SILVA, Rodrigo da Guia. (Org.). O Direito Civil na Era da Inteligência Artificial. 1ed.São Paulo: Thomson Reuters Brasil, 2020, v. 1, p. 585-608.

ROBL FILHO, Ilton Norberto. **Direito, Intimidade e Vida privada.** Paradoxos Jurídicos e Sociais na Sociedade Pós-Moralista e Hipermoderna. Ed. Juruá. 2010. 190 p.

ROBL FILHO, Ilton Norberto. **Intimidade e vida privada**: passado, presente e futuro. 7 jan. 2023. **Conjur**. Disponível em: https://www.conjur.com.br/2023-jan-07/observatorio-constitucional-intimidade-vida- privada-passado-presente-futuro#author. Acesso em: 16 set 2023.

ROSENVALD, N.; BRAGA NETTO, F.P. Responsabilidade Civil: teoria geral. Indaiatuba, SP: Editora Foco, 2024. p. 1.264.

ROSENVALD, N. Responsabilidade civil: compensar, punir e restituir. **Revista IBERC**, Belo Horizonte, v. 2, n. 2, 2019. Disponível em: https://revistaiberc.emnuvens.com.br/iberc/article/view/ 48. Acesso em 21 maio 2023.

ROSENVALD, N. A LGPD e a despersonalização da personalidade. 20 ago. 2021. **Migalhas de IA e Proteção de dados**. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/350374/a-lgpd-e-a-despersonalizacao-da-personalidade. Acesso em 24 set 2023

ROSENVALD, N.; FALEIROS JÚNIOR, J. L. de M. Answerability e seus reflexos para a responsabilização civil. **Revista IBERC**, Belo Horizonte, v. 6, n. 3, p. IV-X, 2023. Disponível em: https://revistaiberc.responsabilidadecivil.org/iberc/article/view/284. Acesso em: 3 maio. 2024.

RUSSEL, Stuart Jonathan; NORVIG, Peter. **Inteligência artificial**. 3. ed. Tradução de Regina Célia Smile. Rio de Janeiro Elsevier, 2013. p. 605.

SANTANA, Agatha Gonçalves; MEIRELLES, Arthur. A responsabilidade civil envolvendo inteligências artificiais em carros autônomos: repercussões no Código de Defesa do Consumidor. **Civilistica.com**. Rio de Janeiro, a. 11, n. 2, 2022. Disponível em: http://civilistica.com/a- responsabilidade-civil-envolvendo/. Acesso em: 01 nov. 2023.

SANTOS, Bruno Henrique Silva. Precaução e prevenção no direito à saúde: âmbitos de incidência e sua aplicação pelo STF. **Revista Direito Hoje** – Emagis. Escola da Magistratura do TRF da 4ª Região. 2020. Disponível em: https://www.trf4.jus.br/trf4/co_ntrolador.php?acao=pagina_visualizar&id_pagina=2104. Acesso em: 2 mai. 2024.

SANTOS, Romualdo Baptista dos. Responsibility, liability, *accountability* e answerability: sistema articulado de responsabilidade civil em face das tecnologias digitais. **Revista de Direito da Responsabilidade – RDR**. 2023. Disponível em: https://www.academia.edu/96687271/RESPONSIBILITY_LIABILITY_ACCOUNTABILITY_E_ANSWERABILITY_SISTEMA_ARTICULADO_DE_RESPONSABILIDADE_CIVIL_EM_FACE_DAS_TECNOLOGIAS_DIGITAIS?email_work_card=view-paper Acesso em: 28 mai. 2024.

TANASESCU, E. S. On responsibility in public law. Cadernos de Pós-Graduação em Direito: estudos e documentos de trabalho. **Revista da Faculdade de Direito da USP**, São Paulo, n. 1.

SAVATIER, René. **Traité de la Responsabilité Civile em Droit Français**. 10 ed. Paris: LGDJ – R. Pichon e R. Durand-Auzias, 1951.

SCHAEFER, Fernanda. Telessaúde e responsabilidade civil digital na lei 14.510/22. **Migalhas de Responsabilidade Civil**. 14 fev. 2023. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-responsabilidade-civil/381503/telessaude-e-responsabilidade-digital-na-lei-14-510-22 Acesso em: 12 mai. 2024.

SHABBIR, Jahanzaib; ANWER, Tarique. **Artificial intelligence and its role in near future**. Journal of Latex Class Files, v. 14, n. 8, aug. 2015.

SILVA, Gabriela Buarque Pereira. **Responsabilidade civil, riscos e inovação tecnológica: os desafios impostos pela inteligência artificial**/ Gabriela Buarque Pereira Silva. Orientador, Marcos Ehrhardt Júnior. Dissertação (Mestrado em Direito) – Universidade Federal de Alagoas. Faculdade de Direito de Alagoas. Programa de Pós-Graduação em Direito. Maceió, 2021. 140 f.

SHERIFF KD. **Defining Autonomy in the Context of Tort Liability**: Is Machine Learning Indicative of Robotic Responsibility? 2015. Available at SSRN: https://ssrn.com/abstract=2735945 or http://dx.doi.org/10.2139/ssrn.2735945. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2735945 Acesso 11 maio 2024.

SMITH, Jake. **Machine Learning for beginners**: can Machines real like humans?. Kindledition, 2017, p. 82.

STRELKOVA, O. PASICHNYK, O. **Three types of artificial intelligence**. Disponível em: http://eztuir.ztu.edu.ua/jspui/bitstream/123456789/6479/1/142.pdf. Acesso em: 23 mar. 2024.

TĂNĂSESCU, Elena Simina. Comissão de Pós-Graduação da Faculdade de Direito da Universidade de São Paulo – USP. On responsibility in public law. Cadernos de Pós-Graduação em Direito: estudos e documentos de trabalho. **Revista da Faculdade de Direito da USP**, São Paulo, n. 1, 2011

TEFFÉ, Chiara Spadaccini; MEDON, Filipe. **Responsabilidade civil e regulação de novas tecnologias: questões acerca da utilização de inteligência artificial na tomada de decisões empresariais**. Disponível em: https://estudosinstitucionais.com/REI/article/view/383/493 Acesso em: 29 set 2023.

TEPEDINO, G.; DA GUIA SILVA, R. Desafios da inteligência artificial em matéria de responsabilidade civil. **Revista Brasileira de Direito Civil**, *[S. l.]*, v. 21, n. 03, p. 61, 2019. Disponível em: https://rbdcivil.emnuvens.com.br/rbdc/article/view/465. Acesso em: 20 set. 2023.

TEPEDINO, Gustavo; SILVA, Rodrigo da Guia. **Inteligência Artificial e elementos da responsabilidade civil**. In: FRAZÃO, Ana; MULHOLLAND, Caitlin (Coord.). Inteligência artificial e direito: ética, regulação e responsabilidade. Editora Revista dos Tribunais, 2019.

TEPEDINO, Gustavo. **As tecnologias e a renovação do Direito Civil**. Publicado em 12 de junho de 2019. Disponível em: http://www.oabrj.org.br/colunistas/gustavo-tepedino/as-

tecnologias-renovacao-direito-civil?fbclid=IwAR1PumT-lccIeKgJQzAbrV6o1Odgqzh1CkrAva5UsHbu3RWyYgTkrn2V9M. Acesso em:28 ago. 2023.

The White House, FACT SHEET: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial I ntelligence (Washington D.C, October 2023). Disponível em: https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president- biden-issues-executive-order-on-safe-secure-and-trustworthy-ar. Acesso em: 9 nov. 2023.

TRIMARCHI, Pietro. Rischio e responsabilità oggetiva. **Milano**: A. Giuffrè, 1961, p.13.

TURING, Alan. **Computing machinery and intelligence.** Mind. V. 59, p. 433-460, 1950.

TURNER, Jacob. **Robot Rules**: Regulating Artificial Intelligence. GF Books, Inc. 2018. 377 p.
UK governament. Disponível em: https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023. Acesso em: 11 nov. 2023.

UNZELTE, Carolina. **Marco Legal da IA**: entenda os principais pontos do texto preliminar. Jota. 2024. Disponível em: https://www.jota.info/legislativo/marco-legal-da-ia-entenda-os-principais-pontos-do-texto-preliminar-08052024?utm_campaign=jota_info__ultimas_noticias__destaques__852024&utm_medium=email&utm_source=RD+Station. Acesso em: 12 mai 2024.

VIDAL, Sebástian. Tipos de robôs: origem, características e muito mais. 2024. **Tecnobits**. Disponível em: https://tecnobits.com/pt/tipos-de-caracter%C3%ADsticas-de-origem-de-rob%C3%B4s-e-muito-mais/. Acesso em: 17 mai. 2024.

XUETING, GE. Research on artificial intelligence tort liability. T**he Frontiers of Society, Science and Technology (2022)** v. 4, Issue 9: 21-25. Disponível em: https://doi.org/10.25236/FSST.2022.040905. Acesso em: 14 jan. 2024.

ZUBOFF, Shoshana. (2019). **The age of surveillance capitalism**. The fight for the future at the new frontier of power. London: Profile Books.

WIMMER, Miriam e DONEDA, Danilo. “Falhas de IA” e a Intervenção humana em decisões automatizadas: parâmetros para a legitimação pela humanização. **Direito Público**, [S. l.], v. 18, n. 100, 2022. DOI: 10.11117/rdp.v18i100.6119. Disponível em: https://www.portaldeperiodico s.idp.edu.br/direitopublico/article/view/6119. Acesso em: 13 mai. 2023.

WEDY, Gabriel de Jesus Tedesco. Os elementos constitutivos do princípio da precaução e a sua diferenciação com o princípio da prevenção. **Revista de Doutrina da 4ª Região**, Porto Alegre, n. 68, out. 2015. Disponível em: https://revistadoutrina.trf4.jus.br/artigos/edicao068/Gabriel_ Wedy.html. Acesso em: 2 mai. 2024.