

# INTELIGÊNCIA ARTIFICIAL E RISCOS: A PRECAUÇÃO COMO FUNDAMENTO E PRINCÍPIO REGULADOR PARA O DESENVOLVIMENTO E IMPLEMENTAÇÃO DE NOVAS TECNOLOGIAS

Ana Fachini<sup>1</sup>

Rosilene Caetano Lago<sup>2</sup>

Rudinei José Ortigara<sup>3</sup>

## RESUMO

O presente artigo tem como objetivo compreender e verificar o desenvolvimento e a importância que a implementação de sistemas de IA adquirem na sociedade atual ante potenciais riscos cientificamente incertos e imprevisos, bem como de analisar a relevância do princípio da precaução como fundamento para a governança de riscos. O problema central se consubstancia em relação à responsabilidade e as possibilidades de controle dos riscos em contextos de incerteza, já que incertos e imprevisíveis. A hipótese é a de que neste contexto a precaução pode ser adotada como fundamento e princípio regulador para o desenvolvimento e implementação de novas tecnologias, ampliando-se perspectivas de controle e de segurança antecipados, de modo a evitar impactos incertos e indesejados. Discute-se elementos dos riscos e sua regulação presentes no Regulamento da União Europeia sobre Inteligência Artificial e do Projeto de Lei Brasileiro de n.º 2338/2023, por serem propostas recentes. Utiliza-se do método dedutivo-dialético e do procedimento bibliográfico para o desenvolvimento da pesquisa.

**Palavras-chave:** Inteligência Artificial. Risco. Incertezas. Regulamentação. Princípio da Precaução.

<sup>1</sup> Acadêmica do 7º período do curso de Direito da FAE Centro Universitário. Bolsista do Programa de Apoio à Iniciação Científica (PAIC 2023/2024). *E-mail:* ana.fachini@mail.fae.edu.

<sup>2</sup> Acadêmica do 9º período do curso de Direito da FAE Centro Universitário. Voluntária do Programa de Apoio à Iniciação Científica (PAIC 2023/2024). *E-mail:* rosilene.lago@mail.fae.edu

<sup>3</sup> Professor orientador. Doutor em Direito pelo Pontifícia Universidade Católica do Paraná. Professor da FAE Centro Universitário.

## INTRODUÇÃO

Em novembro de 2023 emergiu no mundo uma nova tecnologia de inteligência artificial extremamente sofisticada, que se tornou a plataforma com mais rápido crescimento em usuários da história; em apenas dois meses atingiu a marca de 100 milhões de usuários ativos. Tratava-se do ChatGpt<sup>4</sup>. Apesar de específica à execução de uma única atividade, ela chamou a atenção para as potencialidades do desenvolvimento, implementação e uso de tecnologias de inteligência artificial – IA.

Embora o destaque à esta tecnologia, na atualidade há diversas e variadas aplicações de sistemas de IA, de modo que se torna difícil compreender o funcionamento da sociedade separado de suas utilizações. A tendência é a aprofundamento da dependência entre a sociedade e as tecnologias de IA. No entanto, apesar dos enormes benefícios tem-se chamado a atenção aos potenciais riscos da implementação. Riscos que podem ser previsíveis e, portanto, controláveis, como também imprevisíveis e incertos, derivados de usos intencionais ou não intencionais e de efeitos não previstos.

É o contexto dos riscos incertos, nem sempre calculáveis e previsíveis cientificamente, que demandam maior atenção ante o potencial de prejuízos sociais extensos e irreversíveis. E é justamente sobre os desafios e potencialidades de controlabilidade deles que se encontra o enfoque e discussão deste trabalho. O problema central a ser debatido se consubstancia em relação às possibilidades de controle dos riscos em contextos de incerteza em relação ao potencial risco de impactos futuros e não totalmente previsíveis, o papel de responsabilidade dos fornecedores e desenvolvedores, bem como de perspectivas de garantia de segurança, em termos de evitamento de impactos indesejados para e pela sociedade.

A hipótese inicial é a de que no contexto de potenciais riscos incertos e imprevisíveis a precaução se demonstra adequada para ser adotada como fundamento e princípio regulador para o desenvolvimento e implementação de novas tecnologias, ampliando-se perspectivas de governança, controle de riscos e de ampliação da segurança por parte dos fornecedores, de modo a evitar impactos sociais incertos e indesejados. De modo geral, o presente estudo objetiva compreender e verificar o desenvolvimento e a importância que a implementação de sistemas de IA adquirem na sociedade atual, bem como, diante de potenciais riscos incertos e imprevisíveis, analisar a relevância do princípio da precaução como fundamento para a governança de riscos e do papel da responsabilidade de ação dos fornecedores.

Como perspectiva essencial ao Direito, cabendo a este a discussão sobre a regulamentação da IA, a análise da precaução será delimitada nas propostas normativas

<sup>4</sup> De acordo com a UFRGS (2023), “O ChatGPT é um modelo de linguagem treinado com machine learning. Inteligências artificiais desse tipo recebem uma enorme quantidade de dados e, partindo deles, aprendem a reconhecer padrões — e a replicá-los”. Disponível em: <https://www.ufrgs.br/infabico/chatgpt-se-torna-plataforma-com-crescimento-mais-rapido-da-historia/> Acesso em: 26 jun. 2024.

do Regulamento da União Europeia sobre IA, por ser a principal precursora da regulamentação da matéria no mundo, e do Projeto de Lei Brasileiro de n.º 2338/2023, por ser a proposta mais recente em nível nacional.

De modo a testar a hipótese e de avançar na análise do objetivo geral, utilizar-se-á do método dedutivo-dialético, cujo procedimento será baseado em pesquisas de livros, artigos, legislações e demais publicações concernentes ao desenvolvimento técnico e aos impactos sociais e jurídicos. Como objetivos específicos, buscaremos no primeiro item do desenvolvimento da pesquisa, compreender o que são sistemas de IA e analisar o processo de ambivalência em relação ao seu desenvolvimento e implementação. Na sequência, como segundo objetivo específico, expender sobre os fundamentos dos riscos em relação ao desenvolvimento das tecnologias de IA, o fazendo a partir da compreensão contextual destes na sociedade contemporânea, com base, sobretudo, na teoria da sociedade de risco, do sociólogo Ulrich Beck. Por fim, no último item, desenvolvemos discussão sobre o terceiro objetivo específico, qual seja, o de analisar a aplicabilidade da precaução como princípio regulador para a governança dos riscos incertos e imprevisíveis ante o desenvolvimento e implementação de tecnologias de IA.

## 1 INTELIGÊNCIA ARTIFICIAL E NOVOS DESAFIOS AO DIREITO

Tecnologias de IA podem ser definidas como um campo dentro das áreas da Ciência da Computação responsável por pesquisar e propor a elaboração de dispositivos computacionais, capazes de simular aspectos ou dimensões associadas a habilidades, capacidades e ao intelecto humano, como as de raciocinar, perceber, aprender, tomar decisões e resolver problemas, com base em dados (Silva, 2013). Russell (2013, p. 25) destaca que “máquinas são inteligentes na medida em que suas ações sejam capazes de atingir seus objetivos”<sup>5</sup>. Para isso, Sistemas de IA são programados para funcionar com níveis variados de autonomia e de habilidades, apresentando, inclusive, capacidade

5 Em termos de legislação, a IA Act, instrumento legal que serve de base para a regulamentação do desenvolvimento de tecnologias de inteligência artificial na União Europeia, aprovado em 14 de maio de 2024, pelo Parlamento Europeu, apresenta no artigo 3º conceituação sobre sistemas de tecnologia de inteligência artificial. Nos termos da legislação “Sistema de IA”, um sistema baseado em máquinas concebido para funcionar com níveis de autonomia variáveis, e que pode apresentar capacidade de adaptação após a implantação e que, para objetivos explícitos ou implícitos, e com base nos dados de entrada que recebe, infere a forma de gerar resultados, tais como previsões, conteúdos, recomendações ou decisões que podem influenciar ambientes físicos ou virtuais” Embora no contexto legislativo brasileiro não haja Lei específica a regulamentar o desenvolvimento de tecnologias de IA, há o Projeto de Lei nº 2338/2023. O projeto, a exemplo da legislação europeia, apresenta também uma definição no art. 4º, inc. I: “sistema de inteligência artificial: sistema computacional, com graus diferentes de autonomia, desenhado para inferir como atingir um dado conjunto de objetivos, utilizando abordagens baseadas em aprendizagem de máquina e/ou lógica e representação do conhecimento, por meio de dados de entrada provenientes de máquinas ou humanos, com o objetivo de produzir previsões, recomendações ou decisões que possam influenciar o ambiente virtual ou real”.

de adaptação para o alcance de objetivos programados, gerando resultados a partir de tarefas pré-determinadas.

O desenvolvimento de sistemas de IA está majoritariamente associado a cinco dimensões ou habilidades inerentes à inteligência humana: I. aprendizagem; II. raciocínio; III. solução de problemas; IV. percepção; e V. domínio da linguagem (Archeegas, 2022, p. 19). A partir dessas dimensões, os campos de aplicação são múltiplos e variados<sup>6</sup>, assistindo-se, na atualidade a uma multiplicação de tarefas e possibilidades de afazeres automatizados, de tal modo que alguns autores reconhecem as tecnologias de IA como tecnologia geral e com capacidade de se tornar onnipresente e se aplicar a todos os afazeres humanos (Santaella, 2023).

Em constante evolução, as tecnologias de IA avançam a partir do desenvolvimento de certas técnicas. As predominantes na atualidade são os campos de *machine learning* e de *deep learning*. A primeira, conhecida também como aprendizado de máquina, se dá a partir do desenvolvimento de técnicas e algoritmos que buscam, por meio do processamento de grande volume de dados, imitar, de forma automatizada e eficiente, o modo como os humanos desenvolvem aprendizagem, resolvem problemas e realizam certas tarefas específicas (ENAP, 2020).

Já a técnica de *deep learning*, ou aprendizado profundo de máquinas, se caracteriza pelo desenvolvimento de um campo, na prática, mais avançado que o da *machine learning*. A partir dela sistemas de IA são capazes de aprender e de executar de forma escalável e, em muitos casos, autônoma, tarefas complexas. A técnica utiliza como base uma estrutura de redes neurais artificiais, estabelecendo conexões significativas e profundas, em múltiplas camadas sobrepostas, ao molde das sinapses no cérebro humano, na busca de estabelecer significados e resolver problemas, bem como de propor análises e soluções de tarefas complexas (ENAP, 2020).

Apesar de ser um campo amplo e de variadas aplicações, o desenvolvimento da IA possui uma historicidade, que remonta<sup>7</sup>, de forma geral, à visão pioneira de Allan Turing, nos anos 1950. Em artigo intitulado "*Computing Machinery and Intelligence*"<sup>8</sup>,

<sup>6</sup> Segundo Russell (2021), atualmente sistemas de IA tem-se demonstrado um dos campos de estudo e de aplicação mais promissores, com potencial de redesenhar e revolucionar vários afazeres da sociedade, demonstrando-se como tecnologia altamente disruptiva e impactando todos os setores socioeconômicos.

<sup>7</sup> Embora exista alguns autores que buscam contextualizar os primórdios da contribuição ao desenvolvimento atual das Tecnologias de IA em pensadores antigos, como é o caso de Nils Nilsson (1998), que sugere que os primeiros passos foram dados por Aristóteles, a partir de seus estudos para o desenvolvimento da lógica estruturada e racional, nos limitaremos à referência ao desenvolvimento ocorrido na atualidade.

<sup>8</sup> TURING, Alan. **Computing Machinery and Intelligence**. Mind 49, 433-460, 1950. Disponível em: <https://redirect.cs.umbc.edu/courses/471/papers/turing.pdf>.

Turing questionava se uma máquina poderia alcançar o nível de inteligência de modo a se passar por um humano, enganando-o quando da interação estabelecida de forma escrita. Naquele período ainda não o era possível, mas atualmente essa barreira foi transposta, e sistemas de IA se passam naturalmente por interlocutores humanos, a exemplo do uso de modelos de linguagens naturais, como o Chat-GPT<sup>9</sup>.

Especificamente em relação ao termo “inteligência artificial”, a primeira manifestação se deu em conferência organizada por John McCarthy, em Dartmouth College, intitulado de *Dartmouth Summer Research Project*, no ano de 1956. O evento congregou diversos pesquisadores, cujo objetivo foi o de descobrir como desenvolver máquinas capazes de: I. usar linguagem; II. desenvolver instruções e conceitos; III. apresentar resoluções de problemas ao molde como o fazem humanos; IV. ser capazes de se autodesenvolver e de melhorar sozinhas (Elliott, 2022).

Sistemas de IA passaram a ser de fato um campo concreto e central de pesquisa, apresentando quase que diariamente criações inovadoras. É o caso dos chatbots, conhecidos como assistentes virtuais, como a Siri e a Alexa, e IA generativa<sup>10</sup>, “uma extensão mais recente que pode criar coisas novas em todas as mídias que, até então, eram vistas como exclusivas da inteligência e da criatividade humana: texto, vídeo, áudio e imagens” (Timpone, 2023, p. 3). Um exemplo bastante conhecido e utilizado na atualidade é o Chat GPT, uma IA generativa em massa capaz de gerar textos e informações em linguagem natural, que angariou usuários de forma extraordinária, atingindo 2,4 bilhões de acessos em janeiro de 2024<sup>11</sup>.

Para além dos exemplos citados, e de forma não exaustiva, alguns contextos de aplicação de modelos de sistemas de IA na atualidade se destacam: aplicação em e-commerce; entretenimento em geral; internet, redes sociais e aplicativos; tradutor de idiomas; moderação de conteúdo em redes sociais; transporte de cargas e pessoas; saúde; carros inteligentes; automação comercial e industrial em diversos setores; reconhecimento biométrico, criação de conteúdos<sup>12</sup>; dentre outros.

Devido às potencialidades de aplicação, cada vez as tecnologias e sistemas de IA ocupam espaço e presença significativos na sociedade, que está cada vez mais

<sup>9</sup> Recentemente foi divulgada a notícia de que um modelo de IA passou o teste de Turing. Trata-se do modelo GPT4, da OpenAI, que foi identificado como um interlocutor humano em 54% das vezes. Sugere-se a leitura do seguinte: <https://epocanegocios.globo.com/inteligencia-artificial/noticia/2024/06/chatgpt-passa-em-teste-de-inteligencia-humana-dizem-pesquisadores.ghtml>.

<sup>10</sup> IA Generativa é um campo em rápido avanço que já permite a produção automatizada de conteúdo textual, gráfico, sonoro e audiovisual de alta qualidade (Franganillo, 2023).

<sup>11</sup> Notícia fornecida por Murilo Tunholi, para a Revista Giz Brasil, em março de 2024.

<sup>12</sup> CHIAVONE, Tayrone Marquesini. **Sociedade De Risco Digital**: O Princípio da Precaução na Regulação da Inteligência Artificial. São Paulo: Editora Dialética, 2023. p. 56-58.

ambientada em um mundo permeado por tecnologias e inovações constantes. Afinal, a maioria das pessoas já obteve a experiência, ou ao menos teve notícia, de como é dirigir um carro sem necessariamente ter um condutor humano. Ou ainda, como é pagar compras no supermercado sem o auxílio de um operador de caixa. E até de assinar e acessar serviços de streaming, ou outros serviços digitais, e de encontrar sugestões dadas pelo próprio algoritmo, bem como de ferramentas produtivas e automatizadas, como geração de textos, imagens e vídeos, dentre outros<sup>13</sup>.

De tão ampla aplicação, as apostas nos benefícios se espalham tanto em aplicações públicas, focando-se na eficiência da gestão pública e nos benefícios sociais, quanto privadas, focados especialmente em aspectos de ganhos econômico e de produtividade. A exemplo, a União Europeia (2023) pontua que os principais impactos positivos da implementação de sistemas de IA à humanidade se estendem desde questões sociais, passando por ambientais, econômicas e culturais, dentre outros, quando de sua utilização como ferramenta para otimização de processos, personalização na prestação de serviços e competitividade e eficiência econômica<sup>14</sup>.

Em campo específico ao jurídico, até mesmo o poder judiciário vem apostando no desenvolvimento e implementação de sistemas de IA. Segundo o Ministro Barroso (2024), presidente do Supremo Tribunal Federal (STF), a Inteligência Artificial pode ser adotada com a finalidade de acelerar o sistema de Justiça, processando muitas informações, gerando despachos simples, e até mesmo auxiliando em processos de análise de provas e demais dados quando da escrita de sentenças; porém, ressalva a necessidade de se considerar a supervisão humana em todas as etapas da aplicação e da utilização de tais sistemas.

Assiste-se, nos últimos anos, uma espécie de “euforia” em relação ao desenvolvimento, uso e aplicação de tecnologias de IA, atribuindo-se a elas o potencial de fonte de solução para todos os males da sociedade (Han, 2022), inclusive, atribuindo-lhe uma perspectiva, em certo sentido religioso, de redentora e salvadora da humanidade (Harari, 2016). No entanto, igualmente é crescente a tendência de alertas de preocupação do uso, aplicação e implementação, pois, apesar dos benefícios, novos riscos ou consequências negativas vêm sendo percebidos, alguns até mesmo

<sup>13</sup> Essas funções representam alguns exemplos de aplicação de sistemas de IA já presentes, que podem ser definidos como “um braço da computação cujo objetivo primordial é desenvolver programas computacionais capazes de automatizar ações inteligentes” (Archeegas, 2022, p. 13).

<sup>14</sup> A inteligência artificial (IA) é uma família de tecnologias em rápida evolução capaz de oferecer um vasto conjunto de benefícios econômicos e sociais a todo o leque de indústrias e atividades sociais. Ao melhorar as previsões, otimizar as operações e a afetação de recursos e personalizar o fornecimento dos serviços, a utilização da inteligência artificial pode contribuir para resultados benéficos para a sociedade e o ambiente e conceder vantagens competitivas às empresas e à economia europeia. (União Europeia, 2023a).

nem previstos quando do início de seu uso. A análise e atenção aos riscos é central na discussão dos usos de tecnologias de IA, vez que são marcadamente transpassadas pela condição de ambivalência; ao mesmo tempo em que promessas são grandes, há que se atentar aos riscos reais e potenciais (Jonas, 2007).

Estamos experimentando a concretização latente de diversos impactos negativos da IA na sociedade, a exemplo de: reprodução de vieses discriminatórios, com riscos potenciais à plena implementação de Direitos Humanos, pois sistemas são alimentadas, mesmo que de forma indireta, com dados apresentando perspectivas preconceituosas<sup>15</sup>; classificação de risco e crédito financeiro, com negativas automatizadas; advento e presença cada vez maior, com tendência de se tornar massiva no futuro, do desemprego e da substituição de postos de trabalho; e por riscos concretos à democracia liberal<sup>16</sup>, prejudicando o debate político e favorecendo a desinformação, através da disseminação de notícias “fabricadas” ou falsas, e ante a avançada capacidade de criação de *deep fakes*, com áudios, imagens e vídeos falsos extremamente realistas; violações de privacidade e segurança<sup>17</sup>; dentre outros.

Em face dos riscos e do reconhecimento de que a implementação de sistemas de IA vem tomando fortes proporções, acarretando grandes transformações sociais, com impactos profundos, o direito começa a dar os primeiros passos para regrá-los. Países e regiões como os Estados Unidos, Reino Unido, China, União Europeia de Brasil, estão mobilizando discussões e até mesmo propostas de regulamentação a respeito do assunto. Destaca-se a União Europeia, que foi pioneira ao estabelecer regras, as primeiras do mundo, sobre o desenvolvimento e uso de inteligência artificial. O AI Act (ou Regulamento da União Europeia sobre Inteligência Artificial) foi proposto pela Comissão Europeia em abril de 2021 e aprovado pelo Parlamento Europeu e pelo Conselho da União Europeia no dia 14 de maio de 2024.

O objetivo do AI Act é o de assegurar um ambiente seguro para todos, cuja implementação de sistemas de IA garanta a não violação de direitos fundamentais e de princípios éticos, gerando confiança e ambiente regrado para a ação das empresas

<sup>15</sup> Um exemplo é o apresentado por Cathy O’Neil, em seu livro *Algoritmos de Destruição em Massa*, no qual a autora explica de forma singular o ciclo reatualizativo dos processos discriminatórios gerados pela implementação de sistemas de IA quando alimentados por dados enviesados para o combate de práticas criminosas, e até na aplicação de dosimetria ou progressão da pena, cujos resultados automatizados tendem a serem aplicados de forma mais rigorosa à pessoas provenientes a de certas regiões previamente classificadas de maior risco, bem como da cor da pele. Para aprofundamento, sugere-se a leitura do seguinte: O’NEIL, Cathy. *Algoritmos de Destruição em Massa: Como o Big Data aumenta a desigualdade e ameaça a Democracia*. 1. ed. Santo André: Rua do Sabão, 2020.

<sup>16</sup> Sobre estes dois riscos, para aprofundamento indica-se a leitura da seguinte obra: HARARI, Yuval Noah. *21 lições para o século 21*. São Paulo: Companhia das Letras, 2018.

<sup>17</sup> Impactos negativos da IA reconhecidos por Bernard Marr, em matéria para Forbes Tech, em junho de 2023.

e o cuidado em relação aos potenciais impactos negativos e indesejados para a população, vulnerável no contexto de riscos<sup>18</sup>. O Regulamento classifica os riscos no desenvolvimento, implementação e uso de sistemas de IA quanto ao seguinte: a) risco inaceitável, que engloba práticas de inteligência artificial estritamente proibidas; b) risco elevado (alto), que são sistemas que apresentam impactos substancialmente prejudiciais à saúde, segurança e direitos fundamentais e, por isso, devem ser aplicados mediante observância de requisitos rigorosos de transparência, qualidade de dados, dentre outros; e, por fim, as de c) risco baixo (mínimo), que não se enquadram nas categorias anteriores e, por isso, aplicam-se regras mais leves e proporcionais.

No Brasil, a discussão do tema também está em voga, contexto que desembocou, inclusive, em projeto de Lei recente, elaborado por juristas, de nº 2338 de 2023, e assinado pelo Senador Rodrigo Pacheco<sup>19</sup>. O projeto pretende, conforme sua justificativa, proteger os direitos fundamentais das pessoas, normalmente as mais afetadas pela IA, e criar um sistema de governança que ofereça segurança jurídica para promover a inovação e o avanço tecnológico. Em relação aos riscos, o projeto apresenta categorização em: a) risco excessivo e b) alto risco; ficando a cargo dos agentes de IA estabelecerem estruturas de avaliação preliminar e de governança, com desenvolvimento de processos internos aptos a garantir a segurança dos sistemas e ao atendimento dos direitos de pessoas afetadas (art. 17). Este processo deve ser adotado previamente à introdução ou uso da tecnologia no mercado pelo fornecedor, e sendo desta a responsabilidade pela classificação do grau de risco e da garantia da segurança esperada (art. 13).

Um ponto fundamental e distintivo do projeto de Lei Brasileiro em relação ao Regulamento aprovado pelo Parlamento Europeu é que ele avança em relação aos riscos, prevendo dever de cuidado do fornecedor não só em relação aos previsíveis, mas também aos prováveis, potenciais ou incertos. Assim, no desenvolvimento, implementação e uso de sistemas de IA a atenção aos riscos deve se dar não só aos previsíveis ou calculáveis, mas também aos sistêmicos, derivados de usos intencionais ou não, e de efeitos não totalmente previstos, porém prováveis (art. 3º), levando-se em consideração os impactos gerais, inclusive dos com evidências incipientes, incompletas ou especulativas, visto que, nestes casos, riscos concretizados em danos podem ser de difícil reversão ou irreversíveis (art. 24, §2º).

Em termos do desenvolvimento de sistemas de IA, as razões para a preocupação são variadas e se estendem para além do domínio do conhecido e do previsível, marcando-se pelo

<sup>18</sup> A proposta tem como base os valores e os direitos fundamentais da UE e pretende dar às pessoas e a outros utilizadores a confiança necessária para adotarem soluções baseadas em IA, ao mesmo tempo que incentiva as empresas para que as desenvolvam. A inteligência artificial deve ser uma ferramenta ao serviço das pessoas e uma força positiva para a sociedade com o objetivo final de aumentar o bem-estar dos seres humanos (União Europeia, 2023a).

<sup>19</sup> Avulso do PL 2338/2023, p. 29.

elemento da incerteza. Devido à extensão e classificação das potencialidades e aplicabilidades, cada vez mais é devido se atentar aos potenciais riscos em relação ao desenvolvimento, uso e implementação com o fim de evitamento de impactos negativos e à garantia de segurança para a sociedade, vez que acompanhados da extensão de aplicabilidades e usos vêm os riscos relacionados, base das legislações que buscam regular tais tecnologias.

Devido à dinâmica do desenvolvimento, a implementação e uso de sistemas e tecnologias de IA vêm marcadas pela dinâmica da imprevisibilidade e das incertezas em relação aos resultados e impactos futuros, fugindo à previsibilidade e à calculabilidade. Tal dinâmica foi adotada acertadamente tanto como base quanto como princípio para o desenvolvimento, a implementação e o uso de sistemas de IA pelo Projeto de Lei Brasileiro (art. 3º do Projeto de Lei nº 2338/2023), e, igualmente, como base para o estabelecimento de metodologia da avaliação de impactos, a cargo dos fornecedores (art. 24, §2º do Projeto de Lei nº 2338/2023). Na sequência, discute-se as dimensões, consequências e atenção em relação à dinâmica dos riscos na sociedade contemporânea e ao consequente desenvolvimento das tecnologias de IA.

## **2 ENTRE RISCOS E INCERTEZAS: O CAMINHAR DAS TECNOLOGIAS DE IA**

Uma perspectiva que pode ser relevante para melhor compreender o desenvolvimento e riscos associados ao uso e implementação de tecnologias de IA na sociedade é o fazer a partir da compreensão da dinâmica do desenvolvimento característicos a todas as tecnologias na sociedade contemporânea. A compreensão da tecnologia a partir deste panorama busca ir além da avaliação somente da lei ou de sua aplicação contextual, para compreender a dinâmica do desenvolvimento da tecnologia como elemento estrutural e nodal das próprias dinâmicas sociais e matizes de funcionamento das estruturas alargadas do funcionamento da sociedade. Ante este parâmetro, utilizaremos a teoria da sociedade de risco, desenvolvida por Ulrich Beck<sup>20</sup>, para compreender as dinâmicas dos riscos associados ao desenvolvimento das tecnologias, de modo geral, e como ferramenta e pano de fundo para compreender, igualmente, os riscos associados ao desenvolvimento de sistemas de IA.

Apesar dos aspectos prometeicos, animadores e eufóricos relacionados ao desenvolvimento, uso e aplicação de sistemas de IA, é necessário atentar aos

---

<sup>20</sup> Ulrich Beck (1944 –2015) foi um sociólogo alemão, conhecido pelo desenvolvimento da teoria da sociedade de risco; ela ultrapassa o campo da sociologia, atingindo e se aplicando como perspectiva interpretativa a outros campos do saber, inclusive ao direito. Dentre as perspectivas adotadas pelo autor, o que nos interessa à discussão neste trabalho é a dinâmica da produção moderna de riscos.

potenciais riscos e incertezas. A atenção a esses riscos e incertezas, como reflexo do desenvolvimento e avanços das tecnologias, é essencial na sociedade contemporânea, considerando o extenso potencial das aplicações e a capacidade de modificar diversas estruturas. Os campos de aplicabilidade da IA podem gerar impactos e consequências de alto risco, muitas vezes irreversíveis e irreparáveis quando o dano se materializa, afetando não apenas o presente, mas também o futuro distante (Jonas, 2007). No campo do Direito, essa perspectiva é crucial para considerar possibilidades de regulamentação significativa dos riscos e antecipatória aos danos, visando o desenvolvimento e a implementação segura de sistemas de IA.

Esta é uma questão prática, mas também principiológica, envolvendo discussões relativas ao campo da regulamentação e da aplicabilidade jurídica. Nesse sentido, o Projeto de Lei brasileiro nº 2338 de 2023, que visa regular a IA, acompanha tal preocupação, pois tem como objetivo proteger os direitos fundamentais e garantir a implementação de sistemas seguros e confiáveis, em benefício da pessoa humana, do regime democrático e do desenvolvimento científico e tecnológico (art. 1º). A centralidade da discussão está na compreensão das possibilidades de garantia da segurança e confiabilidade no desenvolvimento de sistemas de IA, considerando não apenas os riscos previsíveis, mas também os incertos e incalculáveis. Condição que demanda dos fornecedores atenção ainda maior às consequências sociais da implementação de novas tecnologias.

Para buscar compreender as dinâmicas dos riscos envoltos à dinâmica do desenvolvimento das tecnologias na sociedade contemporânea essencial se faz a compreensão e caracterização do próprio risco. Conforme elencado no tópico anterior, a existência de potenciais riscos justifica, por si só, a implementação de regulamentação. No entanto, o grande desafio e dificuldade, imposto inclusive ao Direito, é o de identificar e calcular tais riscos (Chiavone, 2023, p. 77). Em questão do Projeto de Lei brasileiro, apresenta categorização dos riscos (Capítulo III) em excessivo e alto risco, ficando a cargo dos agentes e fornecedores de sistemas de IA estabelecerem estruturas preliminares de avaliação e governança dos impactos, inerentes ao próprio desenvolvimento e prévio à implementação.

O mais relevante do Projeto de Lei Brasileiro é o reconhecimento explícito do princípio da precaução como elemento básico, e de observância pelos fornecedores, para avaliação dos impactos, de modo à implementação segura de tecnologias de IA. Este elemento é central pois determina aos fornecedores a obrigação legal de se atentar não só aos riscos previsíveis (excessivos e de alto risco), mas também para os sistêmicos, ou seja, os gerais e não focais e tópicos, condição que engloba mesmo aqueles que sejam incertos, intencionais ou não intencionais, e de efeitos não previstos

(art. 3º, inc. XI, do Projeto de Lei n.º 2338/2023). A dimensão de imprevisibilidade e de incerteza, portanto, passa a ser relevante para a avaliação e elemento de garantia ampliada de segurança.

O elemento contido na legislação é importante, pois, de certo modo, acompanha a dinâmica própria dos riscos ligados ao desenvolvimento de tecnologias na atualidade. A compreensão do risco acompanha os desafios de seu tempo; contemporaneamente ele não significa somente risco, capaz de ser previsto, mensurável e controlável por instrumentos de certeza científica, mas pela incerteza, imprevisibilidade e pela tendência à incontrolabilidade em relação aos resultados danosos, se materializados, sobretudo em termos de impactos espaciais e temporais, além de produzidos pelas dinâmicas próprias e extensão do desenvolvimento tecnológico (Beck, 2015); daí a importância de se pensar elementos garantidores e expansivos da garantia da segurança e da não materialização dos danos sociais em relação ao desenvolvimento, implementação e uso de tecnologias, como as de sistemas de IA.

Frade (2009) destaca as diferentes percepções que o risco tem em várias áreas do conhecimento, em especial a da ciência jurídica, como função reguladora e de segurança diante de fatos novos na sociedade. Explana que o risco está ligado à ideia de obter novos ganhos por meio da ousadia, uma compreensão que se alinha aos contextos atuais e auto-impulsionados do desenvolvimento (Jonas, 2007), ligados à ideia de inovação contínua pela consequente implementação da tecnologia em desenvolvimento. Porém, a ousadia ganha ares de preocupação em relação aos impactos quando demonstram capacidade (riscos certos e previsíveis, excessivos e de alto risco), ou mesmo possibilidade (riscos incertos e imprevisíveis), de extensos impactos sociais e, mesmo, de destruição da vida na terra (Beck, 2022, p. 25).

Para Beck (2022), o desenvolvimento econômico e industrial é, por si só gerador de riscos; ou seja, os riscos são criados e derivados diretamente das dinâmicas do desenvolvimento atual das tecnologias. Agora há uma diferença da materialização dos riscos em relação às condições sociais anteriores, nas quais eles se assemelhavam a perigos provindos de dinâmicas naturais, como terremotos, furacões, pragas, dentre outros. Daí que na fase atual do desenvolvimento tecnológico se pode afirmar que os riscos são produzidos, e os maiores desafios são emergentes da própria dinâmica e implementação dos sucessos do desenvolvimento da sociedade industrial. As incertezas são frutos das dinâmicas e do sucesso das ciências (Beck, 2022, p. 275), que, uma vez aliadas ao desenvolvimento e proveito puramente econômico, acentuam a possibilidade e a incontrolabilidade da produção de riscos, vez que potenciais impactos sociais são colocados em segundo plano (Chiavone, 2023, p. 31).

Os riscos produzidos, aqueles da fase atual do desenvolvimento tecnológico, divergem dos antigos riscos, produzidos externamente à matriz humana, e que eram um acontecimento facilmente previsível, avaliável e controlável em suas consequências, e geralmente delimitados espacial e temporalmente (Castel, 2005, p. 61). Entretanto, essa não é a apresentação atual do risco, a qual representa ameaças e fenômenos nocivos inteiramente alheios no que diz respeito à dimensão social, e cujas consequências danosas, espacial ou temporal, tendem a ser incalculáveis e imprevisíveis. Neste contexto, a essencialidade caracterizadora da sociedade de risco são as incertezas fabricadas, derivadas da auto-implementação e da impulsividade constante ao desenvolvimento a todo custo, muitas vezes descontrolado (Beck, 2022, p. 33).

No contexto do desenvolvimento, da implementação e do uso de sistemas de IA, os fornecedores estão cada vez mais focados em otimizar processos, aprimorando ao máximo as tecnologias e desenvolvendo sistemas cada vez mais sofisticados; no entanto, este mesmo processo de auto-implementação contínua é geradora de condições de incertezas em relação aos potenciais impactos sociais. Devido à extensibilidade de aplicabilidade desta tecnologia, desde modelos mais simples, como os desenvolvidos para “jogar” determinados e-mails na caixa de spam, até os mais sofisticados, como os capazes de diagnósticos médicos, a aplicação de sistemas de IA possui potencial de implementação quase que ilimitada. Apesar da grande ajuda, várias ameaças já puderam ser detectadas, a exemplo de bugs, falhas de segurança, invasão de privacidade, desinformação, perda de conexão humana, dentre outros<sup>21</sup>.

Alertas mais incisivos têm sido emitidos em relação aos riscos e incertezas do desenvolvimento de etapas futuras. Até o presente momento, e embora altamente eficientes, o desenvolvimento de sistemas de IA possuem escopo de tarefa limitado a uma atividade específica; em termos técnicos, esta etapa tem sido nominada de IA estreita (ANI), a que está condicionada à realização de apenas uma atividade específica para a qual foi programada. Mesmo assim, elas demonstram potenciais de riscos sociais<sup>22</sup>. Para além dela, existem mais duas outras possíveis etapas no desenvolvimento

<sup>21</sup> “I. Falhas (bugs): como qualquer sistema de software apresenta falhas, os sistemas de IA devem ser cuidadosamente testados e validados. II. Segurança (cybersecurity): os sistemas de IA são tão vulneráveis quanto qualquer outro software a ataques cibernéticos. III. Aprendiz de feiticeiro (sorcerer’s apprentice): os sistemas de IA devem raciocinar sobre o que estas pretendem, em vez de executar comandos literalmente. IV. Autonomia compartilhada (shared autonomy): construir esses sistemas colaborativos levanta um quarto conjunto de riscos decorrentes de desafios sobre fluidez de engajamento e clareza sobre estados internos e objetivos dos envolvidos no sistema. Criar sistemas em tempo real onde o controle precisa mudar rapidamente entre as pessoas e os sistemas de IA é difícil; V. Impactos socioeconômicos: Precisamos entender como a IA afeta empregos e economia e garantir sua distribuição justa” (Sichman, 2021).

<sup>22</sup> Outro fato inédito é que pela primeira vez o homem criou algo sob o qual não tem controle; os especialistas não são capazes de afirmar exatamente como as máquinas funcionam e como elas se comportarão no futuro. Decorre desse desconhecimento a origem dos riscos e do imponderável, afetando o futuro da humanidade (Kaufman, 2016, p. 3).

da IA, embora ainda limitadas ao campo teórico.

São a) a IA generalizada (AGI), capaz de executar qualquer tipo de atividade humana, aproximando-se das capacidades cerebrais e de raciocínio humanos, e capaz de desenvolver várias tarefas de modo contextual e relacional, bem como com capacidade de autodesenvolvimento; e b) a superinteligência (ASI), que seria a superação e independência das capacidades cognitivas e mentais humanas, superando-as, e, como tal, com consequências inimagináveis; neste caso, o modelo de inteligência humana pode se tornar “obsoleto” (Barrat, 2013, p. 8-20). Se as ANI já levantam certos alertas de preocupação em relação ao controle, as AGI e as ASI possuem potencialidades alargadas de preocupação, cujas consequências podem ser devastadoras se não houver controle e finalidade de seu desenvolvimento como ferramenta para fins humanos (Torres, 2019).

Torres (2019) destaca que a principal preocupação em relação ao desenvolvimento de tecnologias de IA é a do controle e a da segurança. Legislações como o Regulamento europeu e o Projeto de Lei brasileiro são instrumentos que visam certamente o controle e a garantia de segurança do fornecedor no desenvolvimento de tais tecnologias. No entanto, a própria legislação, ao se deparar com o desafio do controle dos riscos deve se atentar e normatizar os controles a partir das dinâmicas próprias presentes e inerentes à sociedade de risco, essencialmente à condição de incertezas fabricadas e os potenciais impactos extensivos em relação ao tempo e ao espaço. Daí que a condição da precaução se torna essencial como elemento de gestão de riscos sociais e do estabelecimento de responsabilidades dos fornecedores, especialmente em termos de garantia da segurança dos sistemas de IA como passo antecedente à sua implementação e introdução na sociedade.

Em outras palavras, são produtos valiosos advindos de avanços necessários e importantes para o desenvolvimento social, mas que carregam consigo ameaças significativas e incertas, cuja quantificação se mostra desafiadora, acarretando dificuldade em controlá-los. Dada a presença da incerteza em diversas etapas, desde a causa até os efeitos, ela persiste devido a vários motivos: novas tecnologias surgem constantemente, sem uma compreensão completa de seus impactos; muitas vezes, não estudados em contextos reais, além do ambiente controlado do laboratório; e tecnologias já estabelecidas podem revelar, apenas após anos de sua introdução, consequências ambientais ou sociais anteriormente desconhecidas (Aragão, 2008). Daí a importância, em termos de controle e da garantia de segurança, de se estabelecer maiores responsabilidades aos desenvolvedores de tais tecnologias.

A condição de controle e de responsabilidade de segurança é um grande desafio na atualidade, a partir da condição de incertezas fabricadas. Os próprios mecanismos

e ferramentas sociais implementadas para o controle dos riscos, inclusive os da esfera jurídica, foram desenvolvidos em etapa anterior à atual, na qual os riscos eram passíveis de serem quantificados por cálculos probabilísticos (Ferreira, 2008, p. 54-55). O problema é que em condições de incerteza, como o é a condição marcante ao desenvolvimento das tecnologias na atualidade, os riscos passam a ser marcados pela imprevisibilidade e não calculabilidade em relação à extensão e à temporalidade dos impactos, escapando aos instrumentos tradicionais de controle<sup>23</sup>. O risco é o de que ninguém acabe por ser responsabilizado ou se responsabilizando pela produção e distribuição dos riscos sociais e pelos resultados e impactos danosos e negativos (Beck, 2022).

Enfrenta-se uma espécie de panorama invertido, pois, historicamente temos operado sob a premissa de identificar potenciais ameaças associadas a cada ação, e então elaborar estratégias para evitar sua concretização ou, no mínimo, reduzir os impactos significativamente. No entanto, no estágio tecnológico alcançado, inclusive no da IA, essa identificação torna-se cada vez mais difícil, senão impossível, de ser realizada de forma plena, previsível e calculável, o que requer postura diferenciada das ciências, sobretudo da jurídica, que estão sendo chamadas para tomar decisões.

Em face dessa nova fase, a do risco, ou seja, a das incertezas fabricadas e inerentes ao desenvolvimento tecnológico, surge um substrato importante, o princípio da precaução, para se pensar medidas e estratégias de regulação de IA, como forma de lidar com situações de riscos de danos, em condições de incerteza, ou de desconhecimento dos potenciais malefícios e benefícios (Bioni; Luciano, 2019, p. 19). A precaução se insere no sentido de analisar possíveis riscos incertos, pouco ou nada conhecidos, sejam estes globais, retardados ou irreversíveis e de traçar responsabilidades antecipatórias a seu evitamento, a cargo do fornecedor. Em outras palavras, a precaução é considerada como uma garantia ampliada contra riscos potenciais que, de acordo com o estado atual do conhecimento, não podem ser ainda identificados (Silva, 2018, p. 42), potencializando o controle e a garantia de segurança. Daí a importância de se discutir a precaução como fundamento e princípio regulador para o desenvolvimento e implementação de novas tecnologias, o que se fará na sequência.

<sup>23</sup> Segundo Beck (2022, p. 39), Riscos não se esgotam, contudo, em efeitos e danos já ocorridos. Neles, exprimem-se sobretudo um componente futuro. Este baseia-se em parte na extensão futura dos danos atualmente previsíveis e em parte numa perda geral de confiança ou num suposto “amplificador do risco”. Riscos têm, portanto, fundamentalmente que ver com a antecipação, com destruições que ainda não ocorreram, mas que são iminentes, e que, justamente nesse sentido, já são reais hoje.

### 3 REGULAÇÃO DOS RISCOS E O PRINCÍPIO DA PRECAUÇÃO

Regulamentar uma atividade exige a compreensão das dinâmicas envolvidas em seu desenvolvimento. O mesmo se aplica às tecnologias e sistemas de IA, que, como tecnologias de aplicação geral, a regulação se torna condição essencial devido à ampla gama de aplicações e aos possíveis riscos em relação aos impactos sociais. E tal condição significa o mesmo que se atentar aos potenciais danos, previsíveis ou imprevisíveis ou incertos. Portanto, a regulação dos riscos deve levar em consideração o controle tanto dos calculáveis e previsíveis, quanto dos incertos, não mensuráveis e imprevisíveis. Daí que o princípio da precaução<sup>24</sup> indica relevância neste contexto, com o fim de contribuir como ferramental para a regulamentação acerca do controle e da implementação de sistemas seguros e confiáveis.

Em face das dinâmicas dos riscos no desenvolvimento das tecnologias, o direito é “chamado” a atuar como figura responsável sobre a regulamentação e responsabilidade diante do panorama atual. A regulamentação dos riscos, assim, deve se preocupar tanto com riscos quanto com incertezas, de molde a potencializar a segurança e minimizar condições de impactos negativos e indesejáveis em relação ao desenvolvimento, implementação e uso de tecnologias e sistemas de IA<sup>25</sup>. Assim, o risco de danos, na compreensão ampliada que envolve tanto os previsíveis quanto os imprevisíveis, é encarado como o cerne sobre o qual se exerce a missão reguladora, condição que leva a se atentar para a implementação de soluções capazes de restabelecer equilíbrio entre desenvolvimento, o controle de potenciais danosos e a segurança na sociedade.

É certo que ações políticas e de governança, para tomada de decisões, levando em consideração o cenário instável e de incertezas, requerem solução de regulamentação e jurídica que possibilitem não só o controle de riscos previsíveis como os imprevisíveis e incertos, porém, sem que haja paralisação ao desenvolvimento e implementação e desenvolvimento de novas tecnologias. Assim, a implementação deve se dar partir de estratégias de responsabilidade do fornecedor em relação à sua ação, antecipando-se aos potenciais danosos quando da implementação de novas tecnologias, de tal modo a corresponder com a expectativa de segurança esperada

<sup>24</sup> Segundo Chiavone (2023, p. 84), “O princípio da precaução é invocado sempre que inexistir conhecimentos dos riscos potenciais de danos de uma determinada atividade, ou de determinado produto. Os riscos são incertos e não totalmente claros quando mensurados pela ciência. Trata-se então, da administração da incerteza”.

<sup>25</sup> Segundo Aragão, em termos de antecipação dos riscos, pode-se aplicar tanto o princípio da prevenção quanto da precaução. A diferença é que o primeiro se aplica aos riscos calculáveis e mensuráveis, enquanto o segundo aos riscos incertos, mesmo que prováveis. Assim, o primeiro princípio, o da prevenção é um princípio reativo, enquanto o segundo, o da precaução, é um princípio proativo (Aragão, 2013, p. 5).

pela sociedade. A análise é a de que a adoção do princípio da precaução é condição necessária para tal garantia, inclusive o sendo reconhecido no Projeto de Lei n.º 2338/2023<sup>26</sup>, conforme exposto anteriormente.

De acordo com Aragão (2008), o termo precaução, enquanto princípio, surgiu ainda na década de 70 do século passado, sobretudo no campo do direito ambiental, e nos contextos das decorrentes preocupações emergentes em relação ao controle dos impactos das ações humanas no campo ambiental, especialmente como princípio de responsabilidade e “ética do futuro”, devido a ameaças incertas, de grande extensão das ações humanas, sobretudo as relativas à industrialização e implementação de novas tecnologias e seus impactos no meio ambiente, com a intencionalidade de evitamento de catástrofes, estabelecendo responsabilidade de evitamento e de ação antecipatória ante o apontamento de potenciais danos ambientais.

Desde sua origem a condição essencial e estrutural para a aplicação do princípio no campo da garantia da segurança é o das incertezas de danos futuros ante o desenvolvimento das novas tecnologias<sup>27</sup>. As medidas precaucionais, que determinam a responsabilidade do fornecedor, são delimitadas a partir de parâmetros científicos, e não à revelia destes (Aragão, 2013, p. 24). Assim, a condição de incerteza é a da incerteza científica, ou seja, daquela diante da incapacidade de os instrumentos científicos estabelecerem padrões certos e inquestionáveis em relação à segurança da implementação de novas tecnologias e sistemas de IA, mas de que haja indicativos de potencialidade da materialização de danos socioambientais.

A condição de incerteza envolve não a clareza e a probabilidade dos cálculos dos riscos, como ocorre no caso da previsibilidade, mas sua opacidade; ou seja, à condição de impossibilidade de estabelecimento de certezas e de previsibilidades científicas, mas sim de potencialidades e possibilidades<sup>28</sup>. Assim, a incerteza se caracteriza pelo potencial de impactos extensíveis ao futuro, mesmo que potenciais e distantes das ações

<sup>26</sup> Segundo a Autoridade Nacional de Proteção de Dados - ANPD (2023, p. 5), “o PL em discussão, em modelo semelhante ao AI Act europeu, aborda classificações de risco excessivo e risco alto, delimita a regulação consoante os desdobramentos de risco da tecnologia e considera que diferentes níveis de risco justificam diferentes níveis de restrições, garantias e salvaguardas proporcionais. Em algumas circunstâncias, o risco pode ser tão alto que, por precaução, pode ser necessário proibir o desenvolvimento ou uso de aplicativos dessas tecnologias, trazendo, inclusive, o conceito de riscos inaceitáveis”.

<sup>27</sup> Segundo Ortigara (2022, p. 155), “das afirmações e formulações teóricas sobre o princípio da precaução, uma coisa é certa e comum: ele serve como guia em situações e decisões acerca de ações em condições de incerteza em relação a danos potencialmente graves e irreversíveis, provindos de atividades tecnocientíficas”.

<sup>28</sup> Alguns autores, como é o caso de Sustain (2005), formulam pontos de crítica ao princípio da precaução. Um deles é o de que o princípio não seria científico. Esta crítica não possui fundamento consistente, vez que a condição de incertezas e de imprevisibilidade em relação aos resultados de danos potenciais, que permite a aplicação da precaução para o evitamento da ação, deve ser claramente apontada por conhecimentos científicos.

presentes (Jonas, 2007), tornando-os para além de imprevisíveis, retardados em relação à externalidade negativa da ação, bem como com potencialidade de irreversibilidade dos impactos uma vez materializados<sup>29</sup>.

O princípio da precaução, como princípio regulador para o desenvolvimento e implementação de novas tecnologias, marcadas pela condição essencial de incertezas, é essencial à preocupação com a justiça e com o evitamento de riscos irreversíveis, demandando dos fornecedores e desenvolvedores de tecnologias e sistemas de IA novas responsabilidades. Estas se fundam na preocupação alargada e antecipada com a condição de segurança e evitamento de impactos sociais incertos, com a implementação de medidas de antecipação para o evitamento de riscos potenciais e possíveis, muito embora incertos (Chiavone, 2023, p. 83). Se trata de uma ressignificação do instituto da responsabilidade civil, que tradicionalmente exige a materialização do dano para fins de indenização, reparação ou reestabelecimento da condição violada. Trata-se da passagem da necessidade do risco concreto, cuja consequência é estabelecida *ex post facto*, para o da responsabilidade antecipada, para a necessidade de consideração do risco abstrato, estabelecendo-se responsabilidades *ex ante facto* (Freitas; Colombo, 2015). Frisa-se que em condições de riscos incertos e de impactos potencialmente irreversíveis, aguardar a materialização do dano pode ser demasiado temerário na sociedade de risco.

Ao contrário de obstar o desenvolvimento<sup>30</sup>, a precaução visa fornecer parâmetros reforçadores à segurança antecipatória em relação aos potenciais danos do desenvolvimento e da implementação de novas tecnologias a partir de uma abordagem precaucionária, necessária em condições de incerteza, cuja permissividade encontra base no controle e segurança em relação à possibilidade e potencialidade de evitamento de riscos potenciais, sejam os previsíveis, e calculáveis, ou imprevisíveis, mas potenciais (Chiavone, 2023, p. 84), e arrasta a responsabilidade do fornecedor para condições e necessidade de antecipação do dano, já que aguardar sua materialização, em muitas vezes, se demonstra irreversível em relação aos impactos (Burguer Filho, 2018, p. 73).

<sup>29</sup> Segundo Aragão (2008, p. 21), “o princípio da precaução destina-se, sobretudo, a regular os chamados “novos riscos” ambientais que se caracterizam por ser riscos globais, retardados e irreversíveis [...], riscos futuros, que afetarão gerações que ainda não nasceram, é que o princípio da precaução é um princípio de justiça na sua aceção mais clássica. Já na Declaração de Direitos do Homem e do Cidadão, de 1789, se proclamava que “a liberdade consiste em poder fazer tudo o que não prejudique o próximo”. Neste caso, o próximo são as gerações futuras”.

<sup>30</sup> Embora se reconheça que parte da doutrina crê que a aplicação do princípio da precaução se trata de um princípio de medo ou de irracionalidade, devido a um suposto “caráter paralisante”, que prioriza medidas que põe fim ou dificultam o desenvolvimento tecnológico com determinações de “não-fazer” (Sustein, 2005), a oposição que se adota neste artigo é contrária, ou seja, de que se trata de um princípio cuja aplicação potencializa a segurança em relação ao evitamento de impactos indesejados para a sociedade.

Logo, o princípio da precaução se configura enquanto princípio de justiça, cuja implementação e adoção está focada na preservação do amanhã e no evitamento de danos futuros e incertos, porém prováveis, conduta essencial na sociedade de risco. Faz-se referência a ele como uma maneira de “fazer justiça”, porque tem a intencionalidade de proteção daqueles que não possuem condições de proteger a si mesmos, ou possuem vulnerabilidade aumentada, e procura responsabilizar aqueles que têm o dever e o poder de analisar e controlar de forma antecipada os riscos. Neste sentido, é preciso pensar no princípio da precaução a partir do viés de responsabilidade, em que não há uma estagnação diante do progresso tecnológico e sim a garantia de um desenvolvimento científico pautado na responsabilidade do controle e no dever de segurança do fornecedor em relação à governança do risco. Este aspecto é fundamental quando se trata de desenvolvimento, implementação e uso de sistemas de IA, em vista da possibilidade de existência de riscos não só mensuráveis e calculáveis, ou seja, os previsíveis, mas também os incertos e de impactos possíveis, porém não mensuráveis, conforme exposto no tópico anterior.

É quase uma distorção considerar que a aplicação do princípio para o controle dos riscos acarretaria paralisação do avanço das tecnologias. Em termos de regulamentação de tecnologias de IA, o maior desafio atual é contemplar normas que evitem os riscos, enquanto previsíveis, mas também os incertos e potenciais, alargando as exigências de responsabilidade de ação segura dos fornecedores em relação à implementação da tecnologia<sup>31</sup>, mas que, ao mesmo tempo, não inibam o desenvolvimento tecnológico e vice-versa (Kaufman, 2016).

O gerenciamento para implantação de medidas de regulamentação, com a finalidade de impedir práticas dos riscos previsíveis ou não, são desafios impostos às governanças em todo o mundo, com a preocupação de não inibir os avanços e os benefícios ocasionados pela IA. Desta forma, diferentes propostas de regulamentação são estudadas para prevenir e minimizar os danos que possam ser ocasionados pelo uso inadequado da IA, sem deixar de proporcionar inovações tecnológicas. Considera-se que a escolha realizada como proposta de regulação dos riscos exposta no Projeto de Lei brasileiro é acertada, visto que o controle dos riscos não se dá apenas em relação aos riscos previsíveis (excessivos e de alto risco), mas também para os sistêmicos e

<sup>31</sup> “Daí que para alguns o dever de antecipação pode ser lido como um dever de responsabilidade; uma responsabilidade que funda um dever de ação, de antecipação da catástrofe, de modo a evitar danos indesejados, irreversíveis e irreparáveis ao conjunto social, especialmente aos mais vulneráveis. Como responsabilidade, o tomador de decisão assume deveres em relação aos efeitos de sua ação, orientando a ação no sentido da não concretização de efeitos indesejados; o que evoca a ação são os potenciais resultados indesejados e negativos, adotando-se medidas de forma a antecipar-se ao evitamento de danos” (Ortigara, 2022, p. 167-168).

incertos, derivados de escolhas intencionais ou não intencionais dos fornecedores, mesmo que de efeitos não previsíveis e incertos, porém prováveis (art. 3º, inc. XI, do Projeto de Lei n.º 2338/2023).

Como já salientado, os avanços proporcionados pela implementação de tecnologias e sistemas de IA, não podem desconsiderar o alto impacto e riscos existentes, ou seja, o desenvolvimento não deve ser movido por ele mesmo, porém deve, antes, arrastar como elemento de preocupação e de permissividade de continuação a responsabilidade pelo evitamento de resultados e danos à sociedade. Esta condição exige do fornecedor nova postura, a de cautela ante a possibilidade de implementação de nova tecnologia de IA (Moraes, 2011); neste contexto, “a escolha de um regulamento como instrumento jurídico justifica-se pela necessidade de aplicar uniformemente as novas regras, como a definição de inteligência artificial, a proibição de determinadas práticas prejudiciais possibilitadas pela IA e a classificação de determinados sistemas de IA” (Melo, 2022, p. 11).

O princípio da precaução “arrasta” para o presente uma responsabilização que, em moldes tradicionais, como o é a dominante sistemática da responsabilidade civil<sup>32</sup>, só seria possível após a concretização do dano. Ele estabelece responsabilidades antecipatórias, ou seja, *ex ante* ao dano, a cargo do fornecedor, de modo a que este garanta o evitamento e a materialização do dano. Está é condição essencial em tempos de incerteza, pois a implementação de certas tecnologias pode apontar para resultados possíveis, no entanto, não plenamente mensuráveis ou calculáveis, que acarretem danos sociais com resultados, por vezes, catastróficos, graves, irreversíveis e irreparáveis (Ortigara, 2022, p. 155). No caso do Brasil, os parâmetros estão estabelecidos já no art. 1º do Projeto de Lei ao definir que o uso responsável de sistemas de IA tem como objetivo a proteção aos direitos fundamentais e a garantia da implementação de sistemas seguros e confiáveis, em benefício da pessoa humana, ao regime democrático e ao desenvolvimento científico e tecnológico.

No caso do desenvolvimento, implementação e uso de sistemas de IA, a aplicabilidade do princípio da precaução se demonstra essencial como princípio regulador para a avaliação dos impactos e garantidor de maior segurança e controlabilidade dos potenciais riscos. Esta condição é essencial quando se discute as tecnologias de IA, pois, essencialmente marcadas pela condição de ambivalência. Muito embora promessas

<sup>32</sup> A tradicional sistemática da responsabilidade civil, predominante nas relações legais da atualidade, destaca que o advento da responsabilidade civil se caracteriza por quatro elementos, que são: a) conduta, por ação ou omissão; b) culpa, ação com dolo ou negligência; c) dano, a partir de sua materialização em prejuízo sofrido pela vítima; e d) nexa causal, demarcada pela relação de causa e efeito entre a conduta e o dano.

e materializações apontem para grandes realizações e conquistas, não há que se olvidar da condição reflexa dos riscos potenciais e dos cuidados expandidos quando do desenvolvimento implementação e uso de tais tecnologias, sobretudo das incertezas em relação aos danos imprevisíveis e potencialmente irreversíveis.

A responsabilidade pelo evitamento de riscos sociais advindos da implementação de tecnologias e sistemas de IA deve estar a cargo do fornecedor interessado no desenvolvimento, implementação e uso. Este parâmetro geral está estabelecido tanto na Regulamentação Europeia quanto no Projeto de Lei Brasileiro. Conforme os fundamentos apontados acima, no contexto da sociedade de risco a responsabilidade dos fornecedores possui tônica na antecipação dos riscos, especialmente dos imprevisíveis e incertos, porém possíveis, ante os potenciais de danos irreversíveis, de modo a potencializar o controle a segurança necessária.

Em termos de ampliação do controle dos riscos e da garantia da segurança, entendemos que acertadamente o Projeto de Lei brasileiro que dispõe sobre o uso de tecnologias de IA acertadamente previu de forma clara a precaução tanto como princípio para mitigação de riscos cujos efeitos sejam imprevisíveis e incertos (art. 2º, Inc. XI), como fundamento para metodologia da avaliação de impactos, sobretudo quando da implementação de sistemas de inteligência artificial que possam gerar impactos irreversíveis ou de difícil reversão, atentando-se o fornecedor para evidências incipientes, incompletas ou mesmo especulativas (art. 24, §2º).

A aplicação da precaução como princípio regulador para o desenvolvimento e implementação de tecnologias de IA contribui para o controle de riscos e para a ampliação da garantia de segurança da sociedade. No contexto do desenvolvimento tecnológica na sociedade de risco, no qual se insere as IA, não basta apenas que o fornecedor e implementador de sistemas de IA aja somente a partir do princípio da prevenção, ou seja, que tome decisões de evitamento de riscos certos ou previsíveis, ou que se estabeleça sua responsabilidade após a efetivação do dano. É preciso uma mudança paradigmática na gestão da incerteza, incorporada à regulação, abrangendo também o evitamento de riscos incertos e hipotéticos<sup>33</sup>. O que só é possível através da precaução, que tem a capacidade de lidar com riscos possíveis ou potenciais, antes mesmo de qualquer certeza científica, porém potencial (Aragão, 2008).

<sup>33</sup> Segundo Ortigara (2022, p. 162) “é certo que a precaução é exigência e fundamento de ação e antecipação do dano incerto, de modo a evitar danos futuros graves, irreversíveis e irreparáveis, de modo a enriquecer o dever de prevenção. O dever de prevenção, assim, se desdobra para sua devida efetivação, contempla tanto a previsão quanto a precaução, a depender do tipo de risco ao qual o fornecedor se depara e demanda posturas e tomadas de decisão adequadas e complementares a cada situação”.

## CONSIDERAÇÕES FINAIS

A pesquisa objetivou compreender e verificar o desenvolvimento e a importância que a implementação de sistemas de IA adquirem na sociedade atual, bem como, de que diante de potenciais riscos incertos e imprevistos, analisar a relevância do princípio da precaução como fundamento para a governança de riscos. Destacou como problema de pesquisa a análise de como seria possível, em contexto de incerteza, o controle dos riscos do desenvolvimento de sistemas e tecnologias de IA, e o papel de responsabilidade dos fornecedores e dos desenvolvedores, bem como de perspectivas de controle e de garantia de segurança, em termos de evitamento de impactos para a sociedade. Partiu-se da hipótese inicial de que no contexto de potenciais riscos incertos e imprevistos a precaução pode ser adotada como fundamento e princípio regulador para o desenvolvimento e implementação de novas tecnologias, ampliando-se perspectivas de controle e de segurança, de modo a evitar impactos incertos e indesejados.

Ao final a hipótese foi confirmada, no sentido de que ante os riscos do desenvolvimento de tecnologias e sistemas de IA, conforme elementos destacados ao longo da pesquisa, e em contextos de crescente incerteza em relação aos impactos futuros, com potenciais de danos incalculáveis e irreversíveis, a precaução deve ser adotada como fundamento e princípio regulador no cenário geral do desenvolvimento e implementação de novas tecnologias de IA.

Para responder à questão do problema, a pesquisa se baseou em conceitos e teorias que permitiram elencar três pontos principais.

Primeiro: as tecnologias e sistemas de IA permeiam atualmente o contexto existencial de todos, gerando efeitos e impactos sociais, culturais e econômicas, ocasionando benefícios na otimização de processos, em agilizar operações, personalizar serviços, reduzir custos e aumentar a competitividade econômica e empresarial; porém, há riscos envolvidos no desenvolvimento, de tal modo que se faz necessário no contexto atual se atentar a eles. Foi a condição de riscos que motivou o advento tanto do regulamento europeu e do projeto de lei brasileiro, analisados ao longo deste estudo.

Segundo: o risco deve ser elemento e objeto da regulação jurídica, ou seja, um importante fator a ser observado pela regulamentação, permitindo prevenir danos, diante das inovações tecnológicas, como o fizeram tanto a regulação europeia como o projeto de lei brasileiros. Mas para a efetividade da legislação se faz necessária a compreensão do contexto no qual se desenvolvem as tecnologias de inteligência artificial, que é a sociedade de risco, onde as incertezas são fabricadas e cujas consequências e impactos não são totalmente previsíveis, conforme alerta Beck. Esta condição é essencial no desenvolvimento de tecnologias e sistemas de IA.

Terceiro: o princípio da precaução se demonstra essencial para o controle e a garantia da segurança em contextos de incerteza, pois arrasta a responsabilidade dos fornecedores e desenvolvedores de novas tecnologias para o enfoque do evitamento do dano, como responsabilidade *ex ante*, ou seja, preventiva, antes mesmo da inserção na sociedade. Segundo nossa análise, esta condição aparece como destaque no projeto de Lei do Brasil, conforme destacado ao longo deste trabalho, e como fundamento para a governança de riscos, e que exigem um monitoramento constante com o estabelecimento de normas jurídicas a fim de proteger o cidadão para que tenha os seus direitos fundamentais garantidos, sem estagnar os avanços que os sistemas de Inteligência Artificial poderão proporcionar.

Nesta pesquisa limitou-se a compreender a importância da implementação de sistemas de inteligência artificial e a necessidade de sua regulamentação diante da condição dos riscos incertos, no entanto a efetivação do uso dessa legislação e as consequências de responsabilidade civil, em relação aos encargos de uma ação ou omissão diante dos riscos que afete uma pessoa, ou incorporação ou o meio ambiente com o uso da Inteligência Artificial, é uma lacuna que precisará ser desvelada por futuras pesquisas.

## REFERÊNCIAS

- AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS – ANPD. **Análise preliminar do Projeto de Lei nº 2338/2023, que dispõe sobre o uso da Inteligência Artificial**. 2023. Disponível em: [https://www.gov.br/anpd/pt-br/assuntos/noticias/analise-preliminar-do-pl-2338\\_2023-formatado-ascom.pdf](https://www.gov.br/anpd/pt-br/assuntos/noticias/analise-preliminar-do-pl-2338_2023-formatado-ascom.pdf). Acesso em: 10 out. 2024.
- ARAGÃO, A. Princípio da precaução: manual de instruções. **RevCEDOUA**, Coimbra, ano 9, v. 2, n. 22, p. 9-57, fev. 2008. Disponível em: [https://www.researchgate.net/publication/269603897\\_Principio\\_da\\_precaucao\\_manual\\_de\\_instrucoes](https://www.researchgate.net/publication/269603897_Principio_da_precaucao_manual_de_instrucoes). Acesso em: 28 ago. 2023.
- ARHEGAS, J. V.; MAIA, G. O que é inteligência artificial (IA)? Análise em três atos de um conceito em desenvolvimento. **Cadernos Adenauer: Inteligência artificial: aplicações e implicações**, Rio de Janeiro, ano 23, n. 2, p. 9-22, jun. 2022. Disponível em: <https://www.kas.de/documents/265553/265602/KA+Cad+2022-2+vers%C3%A3o+final.pdf/a6ee50d1-b4c5-01b6-6bb2-5500c735a027?t=1656956618327>. Acesso em: 10 out. 2023.
- BARBOSA, X. C. Breve introdução à história da Inteligência Artificial. **Jamaxi**, v. 4, n. 1, 2020.
- BARBOSA, X. C.; BEZERRA, R. F. breve introdução à história da inteligência artificial. **Jamaxi**, v. 4, n. 1, p. 2594-5173, 2020. Disponível em: <https://search.ebscohost.com/login.aspx?direct=true&db=edsbas&AN=edsbas.BFA6F5FA&pt-br&site=eds-live>. Acesso em: 17 out. 2023.
- BARRAT, J. **Our final invention**: artificial intelligence and the end of the human era. Nova York: St. Martin's Griffin, 2013.
- BARROSO, L. R. Inteligência artificial poderá escrever sentenças “em breve”. **Migalhas**, 15 maio 2024. Disponível em: <https://www.migalhas.com.br/quentes/407335/barroso-diz-que-ia-podera-escrever-sentencas-em-breve>. Acesso em: 21 maio 2024.
- BECK, U. **Sociedade de risco**: rumo a uma outra modernidade. Trad. Sebastião Nascimento. São Paulo: Editora 34, 2022.
- BECK, U. **Sociedade de risco mundial**: em busca da segurança perdida. Lisboa: Edições 70, 2015.
- BERGUER FILHO, A. G. **Regulação e governança dos riscos das nanotecnologias**. Belo Horizonte: Arraes, 2018.
- BIONI, B. R.; LUCIANO, M. O princípio da precaução na regulação da inteligência artificial: seriam as leis de proteção de dados o seu portal de entrada. In FRAZÃO, A.; MULHOLLAND, C. **Inteligência artificial e direito**: ética, regulação e responsabilidade. São Paulo: Thomson Reuters Brasil, 2019. p. 207-232.
- BRASIL. Projeto de Lei n. 2338, de 2023. **Dispõe sobre o uso da Inteligência Artificial**. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/157233>. Acesso em: 03 set. 2023.
- CARVALHO, A. C. P. L. Inteligência artificial: riscos, benefícios e uso responsável. **Estudos Avançados**, v. 35, p. 21-36, 2021. Disponível em: <https://www.scielo.br/j/ea/a/ZnKyrCrLVqzhZbXGgXTwDtn/?format=html>. Acesso em: 10 out. 2023.
- CEZAR, F. G.; ABRANTES, P. C. C. Princípio da precaução: considerações epistemológicas sobre o princípio e sua relação com o processo de análise de risco. **Cadernos de Ciência & Tecnologia**, v. 20, n. 2, p. 225-262, 2003. Disponível em: <https://seer.sct.embrapa.br/index.php/cct/article/>

viewFile/8743/4920. Acesso em: 11 out. 2024.

ELLIOTT, A. **Making sense of AI: our algorithmic world**. Sydney: Polity, 2022.

ESCOLA NACIONAL DE ADMINISTRAÇÃO PÚBLICA — ENAP. **Fundamentos de machine learning**. Brasília: 2020. Disponível em: <https://repositorio.enap.gov.br/bitstream/1/7872/3/Mod3%20Fundamentos%20de%20Machine%20Learning.pdf>. Acesso em: 11 out. 2024.

FERREIRA, H. S. **A biossegurança dos organismos transgênicos no direito brasileiro: uma análise fundamentada na teoria da sociedade de risco**. 2008. 370 f. Tese (Doutorado em Direito) — Universidade Federal de Santa Catarina, Florianópolis, 2008. Disponível em: <https://repositorio.ufsc.br/handle/123456789/91741>. Acesso em: 3 jan. 2022.

FERRER, G. G.; MORETTO, A. T. Regulamento europeu sobre inteligência artificial (EU AI Act): pontos de atenção e semelhanças com a proposta de regulação brasileira. **Migalhas**, 29 jul. 2023. Disponível em: <https://www.migalhas.com.br/depeso/390762/regulamento-europeu-sobre-inteligencia-artificial-eu-ai-act>. Acesso em: 03 set. 2023.

FRADE, C. O direito face ao risco. **Revista Crítica de Ciências Sociais**, n. 86, p. 53-72, set. 2009. Disponível em: <https://classroom.google.com/c/NjIwODA3ODUyOTcz/a/NjIwODA5NDgyNTQ0/details>. Acesso em: 28 ago. 2023.

FRANGANILLO, J. La inteligencia artificial generativa y su impacto en la creación de contenidos mediáticos. **Methaodos. Revista de Ciencias Sociales**, v. 11, n. 2, p. 15, 2023. Disponível em: <https://dialnet.unirioja.es/descarga/articulo/9132067.pdf>.

Acesso em: 26 jun. 2024.

FREITAS, V. P.; COLOMBO, S. Da teoria do risco concreto à teoria do risco abstrato na sociedade pós-industrial: um estudo da sua aplicação no âmbito do direito ambiental. **Revista Quaestio Juris**, v. 8, n. 3, p. 1905, 2015.

GEORGI, R. O direito na sociedade de risco. **Revista Opinião Jurídica**, v. 3, n. 5, p. 383-394, 2005.

GUNKEL, D. J.; TRENTO, F. B.; GONÇALVES, D. N. Comunicação e inteligência artificial: novos desafios e oportunidades para a pesquisa em comunicação. **Galáxia**, São Paulo, n. 34, p. 05-19, jan./abr. 2017.

HAN, B.-C. **Não-coisas: reviravoltas do mundo da vida**. Petrópolis: Vozes, 2022.

HARARI, Y. N. **21 lições para o século 21**. São Paulo: Companhia das Letras, 2018.

HARARI, Y. N. **Homo Deus: uma breve história do amanhã**. São Paulo: Companhia das Letras, 2016.

JANCZURA, R. Risco ou vulnerabilidade social? **Textos & Contextos**, Porto Alegre, v. 11, n. 2, p. 301-308, 2012.

JONAS, H. **O princípio responsabilidade**. Rio de Janeiro: Contraponto/PUC-RJ, 2007.

KAUFMAN, D. Inteligência artificial: questões éticas a serem enfrentadas. **Abciber**, São Paulo, v. 9, n. 8, p. 1-16, 2016.

KENSKI, V. M. **Educação e tecnologias: o novo ritmo da informação**. Campinas: Papyrus, 2007.

MARR, B. Os 15 maiores riscos da inteligência artificial. **Forbes**, 2023. Disponível em: <https://forbes.com.br/forbes-tech/2023/06/os-15-maiores-riscos-da-inteligencia-artificial/>. Acesso em: 25 jun. 2024.

‘MEDO, frustrado e constrangido’, diz homem detido por engano em estádio após erro do sistema de reconhecimento facial. **G1**, 21 abr. 2024. Disponível em: <https://g1.globo.com/fantastico/noticia/2024/04/21/medo-frustrado-e-constrangido-diz-homem-detido-por-engano-em-estadio-apos-erro-do-sistema-de-reconhecimento-facial.ghtml>. Acesso em: 25 jun. 2024.

MELO, A. K. A. et al. **Regulação da inteligência artificial**: benchmarking de países selecionados. 2022. Disponível em: <https://repositorio.enap.gov.br/bitstream/1/7419/1/2022.12.08%20-%20Regulacao%20da%20Inteligencia%20Artificial.pdf>. Acesso em: 14 fev. 2024.

MENDES, V. O acirrado debate sobre como regular IA no Brasil. **DW**, 8 out. 2023. Disponível em: <https://www.dw.com/pt-br/o-acirrado-debate-sobre-como-regular-ia-no-brasil/a-67022360>. Acesso em: 15 fev. 2024.

MENDONÇA JUNIOR, C. N.; NUNES, D. J. C. Desafios e oportunidades para a regulação da inteligência artificial: a necessidade de compreensão e mitigação dos riscos da IA. **Revista Contemporânea**, v. 3, n. 7, p. 7753-7785, 2023. Disponível em: <https://ojs.revistacontemporanea.com/ojs/index.php/home/article/download/1146/726>. Acesso em: 10 out. 2023.

MORAES, G. B. A. O princípio da precaução no direito internacional do meio ambiente. 2011. 212 f. Dissertação (Mestrado em Direito), São Paulo, 2011. Disponível em: [https://www.teses.usp.br/teses/disponiveis/2/2135/tde-03092012-111415/publico/MORAES\\_Gabriela\\_Bueno\\_de\\_Almeida\\_Dissertacao\\_de\\_mestrao\\_integral.pdf](https://www.teses.usp.br/teses/disponiveis/2/2135/tde-03092012-111415/publico/MORAES_Gabriela_Bueno_de_Almeida_Dissertacao_de_mestrao_integral.pdf). Acesso em: 11 out. 2024.

NILSSON, N. J. **Artificial intelligence**: a new synthesis. São Francisco: M. Kaufmann, 1998.

O’NEIL, C. **Algoritmos de destruição em massa**: como o Big Data aumenta a desigualdade e ameaça a democracia. Santo André: Rua do Sabão, 2020.

ORTIGARA, R. J. **Da ambivalência das nanotecnologias e da proteção ao consumidor**: a necessária adoção da precaução. 2022. Tese (Doutorado em Direito) — Pontifícia Universidade Católica do Paraná, Curitiba, 2022.

PATRICIO, T. S.; MAGNONI, M. G. M. **Inteligência e Senciência em Chatterbots: Um Estudo Acerca do Jogo da Imitação de Alan Turing**. In: CONGRESSO IBERO-AMERICANO SOBRE ECOLOGIA DOS MEIOS-DA ALDEIA GLOBAL À MOBILIDADE, 1., 2019. **Anais [...]**, 2019.

RUSSELL, S.; NORVIG, P. **Inteligência artificial**. Trad. Regina Célia Simille. Rio de Janeiro: Elsevier, 2013. Disponível em: <https://classroom.google.com/c/NjIwODA3ODUyOTcz/a/NjIwODA5NDgyNTQ0/details>. Acesso em: 12 nov. 2023.

SANTAELLA, L. **Pensar a inteligência artificial**: cultura de plataforma e desafios à criatividade. Belo Horizonte: Fafich/Selo, 2023.

SARGEANT, P. O que é inteligência artificial? Um guia simples para entender a tecnologia. **BBC**, 18 jul. 2023. Disponível em: <https://www.bbc.com/portuguese/resources/idt-74697280-e684-43c5-a782-29e9d11fecf3>. Acesso em: 03 out. 2023.

SICHMAN, J. S. Inteligência Artificial e sociedade: avanços e riscos. **Estudos Avançados**, v. 35, n. 101, jan./abr. 2021. <https://doi.org/10.1590/s0103-4014.2021.35101.004>

SILVA, R. **Inteligência Artificial**. 2013. Disponível em: <http://repositorios.org/jspui/handle/123456789/3737>. Acesso em: 25 jun. 2024.

SILVA, R. F. T.; DIZ, J. B. M. Princípio da precaução: definição de balizas para a prudente aplicação.

**Veredas do Direito**, Belo Horizonte, v. 15, n. 32, p. 39-66, maio/ago. 2018.

SUNSTEIN, C. R. **Laws of Fear: beyond the Precautionary Principle**. Cambridge: Cambridge University Press, 2005.

TIMPONE, R.; GUIDI, M. **Explorando a mudança de cenário da IA: da IA analítica à IA generativa**. Game Changers, 2023. Disponível em: [https://www.ipsos.com/sites/default/files/ct/publication/documents/2023-05/PORTUGUESE\\_20230403-GenerativeAI\\_POV\\_v3.pdf](https://www.ipsos.com/sites/default/files/ct/publication/documents/2023-05/PORTUGUESE_20230403-GenerativeAI_POV_v3.pdf). Acesso em: 03 out. 2023.

TORRES, P. The possibility and risks of artificial general intelligence. **Bulletin of the Atomic Scientists**, Chicago, v. 75, n. 3, p. 105-108, abr./2019.

TUNHOLI, M. Brasil é o 4º país que mais usa ChatGPT no mundo; conheça o top 10. **Gizmodo**, 11 mar. 2024. Disponível em: <https://gizmodo.uol.com.br/brasil-e-o-4o-pais-que-mais-usa-chatgpt-no-mundo-conheca-o-top-10/#:~:text=Dentre%20a%20quantidade%20total%2C%20123,no%20primeiro%20m%C3%AAAs%20de%202024>. Acesso em: 25 jun. 2024.

TURING, A. Computing Machinery and Intelligence. **Mind**, v. 49, p. 433-460, 1950. Disponível em: <https://redirect.cs.umbc.edu/courses/471/papers/turing.pdf>. Acesso em: 11 out. 2024.

UNIÃO EUROPEIA. **Regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de inteligência Artificial (regulamento Inteligência Artificial) e altera determinados atos legislativos da União**. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52021PC0206>. Acesso em: 03 set. 2023a.

UNIÃO EUROPEIA. **O que é a inteligência artificial e como funciona?** Disponível em: <https://www.europarl.europa.eu/news/pt/headlines/society/20200827STO85804/o-que-e-a-inteligencia-artificial-e-como-funciona>. Acesso em: 03 set. 2023b.

ZANIRATO, S. H. et al. Sentidos do risco: interpretações teóricas. **Biblio 3W, Revista Bibliográfica de Geografía y Ciencias Sociales**, v. 13, n. 785, 2008.