DIREITO & TI
ISSN 2447-1097
WWW.DIREITOETI.COM.BR

Avaliações de impacto da Inteligência Artificial: regulação jurídica no Brasil e União Europeia

Artificial Intelligence impact assessments: legal regulation in Brazil and the European Union

Giovanna Voorn Monteiro[1]

Recebido em: 24.02.2025
Aprovado em: 08.08.2025

RESUMO

Avaliações de impacto são instrumentos que permitem identificar e avaliar os potenciais danos dos sistemas de Inteligência Artificial (IA). O presente artigo tem como proposta delinear os requisitos legais do Brasil em contraposição com os da União Europeia (UE) para a implementação das avaliações de impacto relacionadas aos sistemas de IA, à luz do Projeto de Lei nº 2338/2023, aprovado no Senado Federal, da Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e dos Regulamentos 2024/1689 e 2016/679 da UE. O objetivo específico é realizar um estudo qualitativo das avaliações de impacto relacionadas aos sistemas de IA. Para tanto, este trabalho se utiliza do método comparativo com procedimento de análise de conteúdo documental e bibliográfico para se permitir o cotejo entre as regulações. A delimitação conceitual de IA e de avaliações de impacto serão analiticamente abordadas. Identificou-se três tipos de avaliações de impacto: algorítmico; sobre os direitos fundamentais; e sobre a proteção de dados. Embora esta última se restrinja ao tratamento de dados pessoais e à gestão de riscos a liberdades e direitos fundamentais afetados em virtude deste tratamento e as duas primeiras à atividade e à gestão dos riscos do próprio sistema de IA frente aos direitos fundamentais, é verificada uma correlação entre as ferramentas, tanto no seu conteúdo quanto no aspecto metodológico, particularmente quando os sistemas de IA efetuam o tratamento de dados pessoais. Ao final, constata-se as avaliações como importantes mecanismos de governança e segurança que devem ser consideradas pelos agentes de IA.

Palavras-chave: Avaliação de Impacto; Direitos Fundamentais; Inteligência Artificial; Proteção de Dados Pessoais.

ABSTRACT

Impact assessments are tools designed to identify and evaluate the potential risks and harms associated with Artificial Intelligence (AI) systems. This paper aims to delineate

[1] Mestra em Direito pela Pontifícia Universidade Católica de Campinas (2024). Bacharela em Direito, com ênfase em Direito do Estado, pela mesma Instituição (2021). Advogada OAB/SP. Participa do Eixo II- Inovação Regulatória- do Centro Paulista de Estudos da Transição Energética (CPTEn) da UNICAMP, sobretudo no âmbito da regulação jurídica da Inteligência Artificial. E-mail: giovanna.vm2@puccampinas.edu.br. Lattes: http://lattes.cnpq.br/6816920035354686.

the legal requirements in Brazil, in parallel with the European Union (EU), for the implementation of impact assessments related to these systems. The analysis is conducted in light of Bill No. 2338/2023, approved by the brazilian Federal Senate, the General Data Protection Law of Brazil (Law No. 13,709/2018), and EU Regulations 2024/1689 and 2016/679. The specific objective is to undertake a qualitative analysis of impact assessments related to AI systems. To this end, this study employs the comparative method, utilizing documentary and bibliographic content analysis to enable a systematic comparison between the regulations. The conceptual delineation of AI and impact assessments will be analytically examined. Three types of impact assessments have been identified: algorithmic, to fundamental rights, and to data protection. Whereas the latter is limited to the processing of personal data and the management of risks to freedoms and fundamental rights arising from such processing, the first two focus on the activity and risk management of the AI system itself in relation to fundamental rights. Nevertheless, a correlation is observed among these tools, both in terms of content and methodology, particularly when AI systems process personal data. Ultimately, impact assessments are identified as important governance and security mechanisms that must be considered by AI stakeholders.

Keywords: Artificial Intelligence; Fundamental Rights; Impact Assessment; Personal Data Protection.

1 INTRODUÇÃO

A velocidade exponencial do desenvolvimento, utilização de sistemas de Inteligência Artificial (IA) e seus potenciais impactos à pessoa humana têm despertado a atenção do mundo para a sua regulação. A Organização para a Cooperação e Desenvolvimento Econômico (OCDE) publicou em 2019 a Recomendação do seu Conselho de IA elegendo cinco princípios orientadores para a implementação da tecnologia de IA nos seus países membros.[2]

A Organização das Nações Unidas para a Educação, a Ciência e a Cultura (UNESCO, 2021, p.14), por sua vez, publicou sua Recomendação sobre a Ética da IA apresentando como um dos seus objetivos: "fornecer um marco universal de valores, princípios e ações para orientar os Estados na formulação de suas legislações, políticas ou outros instrumentos relativos à IA, em conformidade com o direito internacional."

[2] São eles: 1. Crescimento inclusivo, desenvolvimento sustentável e bem-estar; 2. Respeito pelo Estado de direito, pelos direitos humanos e pelos valores democráticos, incluindo a justiça e a privacidade; 3. Transparência e explicabilidae; 4. Robustez, segurança e proteção; 5. Responsabilidade (OECD, 2019).

Nos termos da 19ª edição do relatório do Fórum Econômico Mundial, *Global Risks Reports*, publicado em 2024, a ascensão da existência de regulações para a implementação da IA no mundo se deve especialmente pela disseminação da desinformação, riscos à cibersegurança e oferecimento de impactos adversos à população despendidos pela tecnologia.

Há exemplos. A predição de acidentes ou mortes pelo sistema de IA, a partir do histórico da pessoa, impacta na precificação e aquisição de planos de saúde; o histórico de compras online impacta na precificação de novos produtos; programas de contratação de trabalhadores, desenvolvidos com a adoção da IA para facilitar a triagem e análise de currículos, impedem a candidatura de pessoas a depender de critérios pré-estabelecidos pelas empresas contratantes (O'Neil, 2020; Franzolin, Monteiro, Laurentis, 2025).

No Brasil, merecem destaque duas normativas inspiradas nos Regulamentos da União Europeia (UE) 2024/1689 (*AI Act*) e 2016/679 (*General Data Protection Regulation* – GDPR), os quais dispõem, respectivamente, sobre a regulação do uso de sistemas de Inteligência Artificial (IA) e a proteção de dados pessoais.

Primeiramente, a Lei Geral de Proteção de Dados (Lei nº 13.709/2018 – LGPD) que disciplina juridicamente sobre a proteção de dados pessoais, informações estas relacionadas à pessoa natural identificada ou identificável (artigo 5º, inciso I da LGPD), bem como o uso e tratamento desses dados[3], nos meios digitais ou físicos, por pessoa natural ou pessoa jurídica de direito público ou privado (artigo 5º da LGPD). Em segundo, o Projeto de Lei (PL) nº 2338/2023 que almeja a implantação do futuro Marco Legal da IA para regular o uso e desenvolvimento de sistemas de IA no país.

Considerando os riscos de danos à pessoa humana, quiçá oferecidos pelos sistemas de IA, os instrumentos normativos exigem dos responsáveis a submissão dos sistemas às avaliações de impacto algorítmico (PL nº 2338/2023) e à produção de relatórios de proteção de dados pessoais (LGPD).

[3] O artigo 5º, inciso X, a LGPD estabelece o tratamento de dados pessoais como: as operações realizadas com dados pessoais que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Entretanto, apesar de preverem, em maior ou menor medida, mecanismos de avaliação de impacto associados ao uso de sistemas de inteligência artificial, ainda se observa uma considerável heterogeneidade quanto: ao escopo de proteção (dados pessoais e impactos amplos de direitos fundamentais); ao momento e grau de obrigatoriedade das avaliações de impacto e à definição e categorização de riscos oferecidos pelos sistemas de IA.

Nesse contexto, este artigo objetiva delimitar os requisitos legais do Brasil e da União Europeia para a execução de avaliações de impacto de sistemas de IA considerando o PL nº 2338/2023, a LGPD, o AI Act e o GDPR. Almeja-se, especificamente, realizar um estudo qualitativo das avaliações de impacto inerentes aos sistemas de IA.

Para tanto, o uso do método comparativo entre as normativas mencionadas no parágrafo anterior é crucial para extrair diferenças e semelhanças que possibilitam a obtenção de *insights* para refinar a abordagem regulatória no Brasil.

O recorte normativo selecionado justifica-se por representar marcos regulatórios contemporâneos que incorporam, em distintas intensidades e abrangências, mecanismos de avaliação de impacto vinculados à proteção de dados pessoais e aos direitos fundamentais. Por apresentarem soluções destinadas à abordagem de problemas semelhantes relacionados ao uso dos sistemas de IA, as normativas selecionadas desempenham a mesma função jurídica (Cury, 2014) razão pela qual, segundo Zweigert e Kötz (1996), são passíveis de comparação jurídica e, portanto, representam o núcleo do presente trabalho.

Normas meramente programáticas ou regulamentações setoriais, ambas de alcance restrito, foram excluídas a fim de garantir a comparabilidade da abordagem regulatória objeto do presente trabalho relativo às avaliações de impacto dos sistemas de IA.

Para a delimitação conceitual de IA e de avaliações de impacto, será empregado o método analítico, que permite a decomposição dos conceitos jurídicos em seus elementos essenciais. Esta abordagem sustentará a análise comparativa viabilizando melhor compreensão dos institutos normativos.

A seleção do material bibliográfico e documental privilegia fontes de reconhecida relevância acadêmica e jurídica, cuidadosamente avaliadas quanto à sua pertinência, atualidade e contribuição para a análise aprofundada do tema em estudo.

Por fim, a seção inicial deste artigo se dedica a apresentar o que se compreende por inteligência artificial e os critérios adotados para identificar e classificar o nível de risco associado aos sistemas de IA no contexto jurídico do PL nº 2338/2023 e do Ato de IA. A seção seguinte dedica-se a abordagem regulatória das avaliações de impacto dos sistemas de IA considerando, sobretudo, o PL nº 2338/2023 do Brasil e o Ato de IA da União Europeia.

Encerra-se, assim, com a dicotomia e similitude entre a abordagem regulatória do Projeto de Lei nº 2338/2023 do Brasil e do Ato de IA da União Europeia no tocante às avaliações de impacto dos sistemas de IA, à vista dos contornos jurídicos da LGPD e GDPR que disciplinam sobre os relatórios (ou avaliações, nos termos do GDPR) de impacto à proteção de dados pessoais.

2 INTELIGÊNCIA ARTIFICIAL: AVALIAÇÃO PRELIMINAR PARA O ENQUADRAMENTO NORMATIVO DO RISCO

O termo Inteligência Artificial (IA) foi cunhado pela primeira vez pelo americano John McCarthy durante a Conferência de Dartmouth de 1956, em New Hampshire. Para o cientista da computação, IA é a parte computacional da capacidade de reproduzir competências semelhantes às humanas e alcançar objetivos envolvendo máquinas.[4] Estas, programadas previamente, fazem o uso de algoritmos[5] que proporcionam a tomada de decisões, predições e interações baseadas nos dados fornecidos de forma automatizada (McCarthy, 1956).

[4] Em entrevista da Universidade de Standford em 2007, John McCarthy responde questões básicas acerca da IA: Q. Yes, but what is intelligence? A. Intelligence is the computational part of the ability to achieve goals in the world. Varying kinds and degrees of intelligence occur in people, many animals and some machines (Monteiro, 2024).

[5] Segundo a autora Voorn Monteiro (2024) um algoritmo é, em suma, um texto que reúne comandos (instruções) a serem executados em uma sequência determinada, comparável a uma receita de bolo composta por um conjunto finito de etapas, pelo sistema computacional que permite realizar uma ação.

Apesar da definição, a Comissão Europeia publicou em 12 de julho de 2024 o Regulamento 2024/1689 (*AI Act* ou, em português, Ato de IA), para tratar da regulação jurídica de sistemas de IA no bloco europeu. Estabeleceu, como objetivo da lei, a colocação em serviço e o uso de sistemas de IA centralizados no ser humano, assegurando a proteção da saúde, da segurança e dos direitos fundamentais consagrados na Carta dos Direitos Fundamentais da União Europeia - CDFUE [6] (União Europeia, 2024).

Para tanto, estabeleceu em seu artigo 3º, n.1 que o sistema de IA é 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 (União Europeia, 2024).

Caminhando no mesmo sentido, o Brasil editou o Projeto de Lei nº 2338/2023, aprovado pelo Senado Federal em 10 de dezembro de 2024 e em tramitação na Câmara dos Deputados, almejando a implantação de um marco legal da IA no país. Se for igualmente aprovado pela Câmara, o projeto será encaminhado para sanção e promulgação pelo Presidente da República, passando a vigorar em todo o país como lei federal após transcorrido o prazo determinado em seu próprio texto para sua vigência (v*acatio legis*).

Na redação atual, o Projeto adotou definição análoga ao artigo 3º, n.1 do AI Act em seu artigo 4º, inciso I. O inciso determina que o sistema de IA é o "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" (Brasil, 2023).

[6] Nos termos do regulamento, destacam-se, nomeadamente, a democracia, o Estado de direito, a proteção do ambiente, a proteção contra os efeitos nocivos dos sistemas de IA na União, e apoio à inovação (União Europeia, 2024).

O dispositivo destaca sobretudo o aprendizado de máquina (*Machine Learning*), uma das principais subáreas[7] da Inteligência Artificial desenvolvida pelo americano Arthur Lee Samuel (1901-1990).[8] Nela, os algoritmos analisam os dados para tomar decisões ou produzir previsões, permitindo a construção e melhora de seu sistema em um processo de aprendizagem automática ante a análise dos dados,[9] sem intervenção humana (Monteiro, 2024; Hossain, 2019).

Os incisos II, III e IV, do mesmo artigo 4º, por sua vez, definem como fornecedor de sistema de IA a pessoa natural ou jurídica, de natureza pública ou privada, que desenvolva um sistema de IA, diretamente ou por encomenda, com vistas a sua colocação no mercado ou a sua aplicação, sob seu próprio nome ou marca, a título oneroso ou gratuito; como operador de sistema de IA a pessoa natural ou jurídica, de natureza pública ou privada, que empregue ou utilize sistema de IA, em seu nome ou benefício, salvo se este for utilizado para atividade pessoal de caráter não profissional; e por fim, como agentes de IA: os fornecedores e operadores desses sistemas.

Apresentado as definições para sua aplicação, o Projeto de Lei segue uma abordagem baseada em riscos utilizada pelo AI Act da União Europeia. Embora não estabelecem regras uníssonas para todos os sistemas de IA existentes, ambas regulações delineiam três tipos de risco que os sistemas oferecem à pessoa humana: risco excessivo ou inaceitável (IA proibidas); alto risco ou risco elevado; e risco baixo ou mínimo[10] (Monteiro, 2024).

[7] A IA é dividida em múltiplas subáreas, dentre elas o processamento de linguagem natural, visão computacional, aprendizado de máquina, robótica, e computação cognitiva (Monteiro, 2024).

[8] O estudo sobre a aplicação do Machine Learning no jogo de damas virtual, dá origem a circulação de uma interpretação da definição de Machine Learning, atribuída como autoria de Samuel. Nela, Machine Learning é o campo de estudo que dá aos computadores a capacidade de aprender sem serem explicitamente programados (Monteiro, 2024).

[9] A matéria-prima utilizada para o funcionamento da IA é o Big Data, quantidade infindável de dados, estruturada através da coleta de dados gerais e pessoais do cidadão, disponíveis no mundo virtual (Monteiro, 2024). Um dado é uma sequência de símbolos quantificados ou quantificáveis (entidade matemática e sintática) que pode ser armazenada e processada por um computador. Representa uma informação (Setzer, 2006).

[10] Cumpre mencionar que em ambas as leis não é apresentado maiores informações ou disposições sobre o risco baixo ou mínimo. Para fins deste trabalho, portanto, a análise será dispensada.

Para cada tipo de risco oferecido para interesses e valores públicos assegurados pelo ordenamento jurídico brasileiro e europeu, que incluem o bem-estar da sociedade (saúde e segurança, por exemplo) e princípios fundamentais que orientam a ação estatal (como liberdade, democracia, igualdade e dignidade humana), obrigações legais são delineadas. Em todos os casos, a determinação do tipo de risco exige o exame do contexto, intenção ou técnica que sustenta um sistema de IA (Monteiro, 2024).

Os sistemas de IA são classificados como aqueles que apresentam um risco excessivo e inaceitável quando oferecidos aos valores do Brasil e União Europeia, valores estes que incluem o respeito pela dignidade humana, a democracia ou a proteção dos direitos fundamentais (Almada, Petit, 2023). Os sistemas de IA que oferecem este tipo de risco, são vedados pelas normas.

A vedação instituída pelas normas inclui as práticas de IA com potencial para manipular indivíduos por meio de técnicas subliminares, além da sua percepção consciente, ou para explorar vulnerabilidades de grupos específicos e vulneráveis, como pessoas com deficiência ou crianças, com a finalidade de modificar substancialmente seu comportamento, resultando em possíveis danos psicológicos ou físicos (Monteiro, 2024).[11]

Diversamente aos riscos excessivos ou inaceitáveis, a classificação de alto risco ou risco elevado não são proibidos e só podem aceder ao mercado do Brasil se estiverem no rol determinado pelos incisos do artigo 17º, cabendo à autoridade competente atualizar a lista dos sistemas de IA de alto risco nos termos do artigo 18º do PL nº 2338/23.

Já na União Europeia, apenas são permitidos aqueles que se enquadrarem no escopo da legislação de segurança de produtos do bloco europeu existente no anexo I; aqueles enumerados no anexo III; e aqueles que integram um componente de segurança de um produto ou são o próprio produto (artigo 6º do AI Act).

No Brasil, para que um sistema de IA esteja em conformidade com as disposições legais e se enquadre em uma das categorias de risco estabelecidas, o artigo 13º do PL nº

[11] Acerca da vulnerabilidade no contexto da IA verificar: WANG, Chenyue, et. al. The artificial intelligence divide: Who is the most vulnerable? **New Media & Society,** [s.l.], v.0, n.0, [s.p.], 2024. Disponível em: https://journals.sagepub.com/doi/epub/10.1177/14614448241232345. Acesso em 10 mar. 2025.

2338/23 impõe ao fornecedor do sistema a obrigação de realizar uma avaliação preliminar, ou seja, uma análise inicial das características e funcionalidades do sistema, com o objetivo de classificar seu grau de risco antes de sua disponibilização no mercado ou implementação em serviços.

Diferentemente do projeto de lei brasileiro, quando se analisa o AI Act da União Europeia, verifica-se que a avaliação preliminar é dispensada pelo bloco europeu. Apesar disso, é exigido do fornecedor e importador a obrigação de submeter o sistema de IA ao procedimento de avaliação de conformidade com o Ato de IA, o qual deverá ser conduzido por um organismo terceiro sempre que se constate que o sistema apresenta um risco elevado (artigos 16º (f), 23º, n.º 1 (a), 42º, 43º e demais disposições do referido Ato).[12]

De maneira oposta a avaliação preliminar, a avaliação da conformidade com o Ato de IA da UE, como o próprio nome sugere, refere-se a um processo formal de verificação, acompanhado e avaliado por um organismo terceiro, para garantir que o sistema de IA esteja em conformidade com os requisitos legais estabelecidos pelo regulamento europeu (Brasil, 2016).

Assim, uma vez classificado como alto risco e a fim de assegurar de forma eficiente a prevenção contra danos, tanto o PL nº 2338/23 quanto o AI Act estabelecem ao fornecedor do sistema de IA de alto risco/risco elevado o dever de submissão do sistema a outro tipo de avaliação: de impacto.

3 AVALIAÇÃO DE IMPACTO: ABORDAGEM REGULATÓRIA DO PROJETO DE LEI N° 2338/23 E AI ACT

[12] Adicionalmente, uma exceção é apresentada pelo Considerando (51). Segundo a disposição orientativa, a classificação de um sistema de IA como de risco elevado não deverá, por si só, implicar que o produto no qual o sistema de IA atua como componente de segurança, ou o próprio sistema de IA enquanto produto, seja considerado como de "risco elevado" conforme os critérios estabelecidos na legislação de harmonização da União Europeia aplicável aos produtos. Tal situação se verifica, nomeadamente, nos casos previstos pelos Regulamentos (UE) 2017/745 e (UE) 2017/746, nos quais é estabelecida a exigência de avaliação da conformidade por terceiros para produtos classificados como de risco médio e elevado.

Em relatório publicado em 2023 pelo *National Institute of Standard Technology* (NIST) dos Estados Unidos, as avaliações de impacto do sistema de IA são definidas como instrumentos que possibilitam auxiliar a compreensão dos impactos, isto é, danos potenciais em contextos específicos (Estados Unidos da América, 2023).

Os agentes, na qualidade de avaliadores de impacto dos sistemas de IA, desempenham a função de analisar e definir requisitos relacionados à responsabilidade e segurança do sistema, mitigar vieses prejudiciais e examinar seus impactos[13]. Devem fornecer expertise técnica que considere fatores humanos, socioculturais e legais (Estados Unidos da América, 2023).[14]

Segundo Watkins, *et. al*. (2021), a expressão "avaliação de impacto de sistemas de IA" é utilizada como um termo abrangente, referindo-se a uma gama de processos e documentação que proporcionam um ponto de partida para mitigar danos potenciais às pessoas singulares e grupos de indivíduos, precipuamente os vulneráveis.[15]

A despeito de não existir ainda um padrão universalmente estabelecido sobre como conduzir essa avaliação[16], a União Europeia em seu artigo 27º do AI Act determinou a obrigatoriedade da realização da avaliação de impacto para sistemas de IA que oferecem um risco elevado aos direitos fundamentais[17] do bloco europeu a ser despendida em momento anterior a implementação desses sistemas.

---

[13] O termo "impacto" invoca uma relação causal: uma ação realizada por uma organização (ou por um sistema sob sua operação) que provoca uma mudança no mundo, tornando-o diferente (Watkins, *et. al*., 2021).

[14] Profissionais que levam em consideração fatores humanos, nos termos do relatório, contribuem com competências e perspectivas multidisciplinares para a compreensão do contexto de uso. Além disso, auxiliam na promoção da diversidade interdisciplinar e demográfica, participam ativamente de processos consultivos, elaboram e analisam a experiência do usuário, conduzem avaliações e testes com foco no ser humano e fornecem subsídios para a realização de análises de impacto (Estados Unidos da América, 2023).

[15] Para um panorama geral sobre vulnerabilidade de grupos de indivíduos, é válido conferir: JANCZURA, Rosane. Risco ou vulnerabilidade social? **Textos & Contextos (Porto Alegre)**, [S. l.], v. 11, n. 2, p. 301–308, 2012. Disponível em: https://revistaseletronicas.pucrs.br/fass/article/view/12173. Acesso em: 10 mar. 2025.

[16] A *International Organization for Standardization* (ISO), estipula na ISO/IEC 42001 a necessidade pelo estabelecimento de um processo de avaliação para determinar o impacto que um sistema de IA exerce sobre indivíduos e sociedades, e atualmente desenvolve a ISO/ IEC 42005, com o intuito de delimitar e estabelecer um padrão a ser adotado nas avaliações de impacto. Entretanto ainda não foi publicado.

[17] Exemplos podem ser extraídos da CDFUE: Dignidade do ser humano (artigo 1°), Direito à integridade do ser humano (artigo 3); Respeito pela vida privada e familiar (artigo 7°); Proteção de Dados Pessoais

Nos termos do artigo 27°, n.1, a obrigação de executar a avaliação de impacto aos direitos fundamentais recai sobre os responsáveis pela implantação de sistemas de IA de risco elevado que sejam organismos de direito público, entidades privadas que prestam serviços públicos e aqueles responsáveis pela implantação de sistemas de IA de risco elevado mencionados no anexo III, ponto 5, alíneas b) e c) do AI Act.

Uma vez abrangidos por essa disposição legal, os responsáveis deverão cumprir a exigência de realizar uma avaliação de impacto que inclua a descrição dos processos do responsável pela implantação em que o sistema de IA de risco elevado seja utilizado de acordo com a sua finalidade prevista, bem como uma descrição do período e a frequência em que o sistema de IA de risco elevado se destina a ser utilizado (artigo 27°, n.1, alíneas (a) e (b) do AI Act).

Igualmente, a avaliação deve abranger as categorias de pessoas singulares e os grupos potencialmente impactados, considerando o contexto específico de utilização do sistema e os riscos específicos de danos a essas categorias. Da mesma forma, deve inserir as medidas a serem tomadas no caso de concretização dos riscos, incluindo as disposições relativas à governação interna e mecanismos de apresentação de queixas; bem como a descrição da aplicação das medidas de supervisão humana de acordo com as instruções de utilização (artigo 27°, n.1, alíneas (c), (d), (e) e (f) do AI Act).

Ao contrário do AI Act da União Europeia empregar o termo "avaliação de impacto sobre direitos fundamentais", o Brasil na implantação do PL nº 2338/2023 optou por impor aos fornecedores de sistemas de IA de alto risco a obrigação de realizar uma "avaliação de impacto algorítmico".

Apesar de terminologias distintas, a avaliação a ser documentada e registrada igualmente se concentra na análise dos potenciais danos que a tecnologia pode oferecer a direitos e bens protegidos pelo ordenamento jurídico brasileiro e europeu. Um exemplo pode ser denotado.

(artigo 8°); Liberdade de pensamento, consciência e da religião (artigo 10°); Liberdade de expressão e da informação (artigo 11°); Liberdade profissional e direito de trabalhar (artigo 15°); entre outros.

Estudantes de regiões pobres de Londres foram prejudicados pela previsão automatizada de notas para o ingresso no ensino superior. Na tentativa de corresponder às distribuições históricas, os algoritmos do sistema de IA aumentaram as notas previstas em escolas pequenas e privadas e reduziram as notas em escolas maiores e administradas pelo Estado, que historicamente atendem uma proporção maior de estudantes de baixa renda (Wachter, Mittelstadt, Russell, 2021).

Como resultado, esses estudantes tiveram suas notas desproporcionalmente reduzidas pelo algoritmo do sistema de IA em comparação com seus colegas, prejudicando seu ingresso no Ensino Superior (Wachter, Mittelstadt, Russell, 2021).

Nessa situação, o dano, o impacto algorítmico ocasionado pelo sistema de determinação de acesso às instituições de ensino prejudicou direitos fundamentais, sobretudo o direito à igualdade (artigo 5º, caput e inciso I da CRFB/88 e Capítulo III da CDFUE) e o direito à educação (artigo 205º e seguintes da CRFB/88 e artigo 14º da CDFUE). Estes são exemplos de impactos que devem ser registrados na avaliação do sistema de IA, seja na União Europeia, seja no Brasil.

Entretanto, ao contrário do artigo 27° do AI Act, o artigo 22° do PL n° 2338, de 2023 exige, sem exceção, que todos os sistemas de IA reputados como de alto risco pela avaliação preliminar sejam submetidos a avaliação de impacto algorítmico. Esta é definida pelo artigo 25° como o "processo iterativo contínuo, executado ao longo de todo o ciclo de vida dos sistemas de IA de alto risco, requeridas atualizações periódicas cuja periodicidade será regulamentada pela autoridade competente."

Igualmente, o PL almeja que as avaliações de impacto algorítmico devem ser realizadas por profissionais com independência funcional que detenham conhecimentos técnicos, científicos e jurídicos necessários para realização de um relatório (artigo 23°, "caput").[18]

Com relação a metodologia, diversamente do AI Act, institui-se no artigo 24° a obrigatoriedade das etapas de preparação; cognição do risco; mitigação dos riscos

[18] No parágrafo único do artigo 23° é estabelecido que cabe à autoridade competente regulamentar os casos nos quais a realização ou auditoria da avaliação de impacto deverá ser conduzida por profissionais ou equipes de profissionais externos ao fornecedor.

encontrados e monitoramento. Muito embora são previstas pelo dispositivo brasileiro, não apresentam detalhamento para a sua implementação, o que confere discricionariedade aos fornecedores dos sistemas de IA dentro das exigências estabelecidas.

Nos termos das alíneas a), b), c), d) e e) do §1º, deve ser considerado e registrado na avaliação de impacto algorítmico os riscos conhecidos e previsíveis à época em que foi desenvolvido, bem como benefícios associados aos sistemas de IA; a probabilidade e a gravidade de consequências adversas, incluindo o esforço para mitigá-las e o número de pessoas potencialmente impactadas; e a lógica de funcionamento do sistema.[19]

Nas alíneas f), g), h), e i), do §1º, deve-se registrar o processo e resultado de testes, avaliações e medidas de mitigação realizadas para verificação de possíveis impactos a direitos, sobretudo para os potenciais impactos discriminatórios; treinamento e ações de conscientização dos riscos; medidas de mitigação, indicação e justificação do risco residual do sistema de IA, acompanhado de testes de controle de qualidade frequentes e medidas de transparência ao público, especialmente aos potenciais usuários do sistema, a respeito dos riscos residuais, principalmente quando envolver alto grau de nocividade ou periculosidade à saúde ou segurança dos usuários, nos termos dos artigos 9º e 10º do Código de Defesa do Consumidor.

4 AVALIAÇÃO DE IMPACTO ALGORÍTMICO EM CONTRASTE COM O RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

O processo decisório algorítmico de um sistema de IA tradicionalmente se inicia com a coleta de dados, informações provenientes da vasta quantidade de dados disponíveis (big data), que fornecem diretrizes e critérios para a sua operabilidade na realização de previsões e tomada de decisões (Monteiro, 2024).

Essas informações reunidas pelos sistemas incluem, por vezes, como apresenta O'Neil (2020), miríade de dados pessoais do usuário, como sua identificação, pagamento,

[19] A lógica de um sistema de IA refere-se ao conjunto de regras, processos e métodos que a IA utiliza para tomar decisões, resolver problemas e aprender com os dados. Essa lógica pode ser baseada em diferentes abordagens, como Lógica Dedutiva e a Lógica Fuzzy, por exemplo (Bauchspiess, 2008).

localização, histórico de saúde, histórico escolar e profissional, histórico de compras e preferências, que podem ser usadas maliciosamente para manipular, rastrear e prever as tendências da pessoa singular ou de grupos de indivíduos.

Alguns impactos potenciais de um vazamento de dados pessoais, segundo a autora Voorn Monteiro (2024), incluem roubo de identidade, exposição de senha, determinação de ativos dos clientes, entre outros que representam uma ameaça em potencial à privacidade da pessoa humana se não for adequadamente protegida.

No Brasil, os direitos à proteção de dados pessoais e à privacidade são previstos como direitos fundamentais (CRFB/88) no artigo 5°. A proteção da "intimidade" e da "vida privada" estão localizadas nos incisos X, XI e XII que tratam da inviolabilidade de casas e sigilo de correspondência, assegurando a privacidade como um direito fundamental para a proteção da pessoa humana. Já a proteção de dados pessoais, foi inserida como o inciso LXXIX do artigo 5° pela Emenda Constitucional nº 115/2022.

Seguindo a CRFB/88, tanto a privacidade quanto a proteção de dados pessoais são igualmente determinados pelo artigo 2°, inciso VIII do Projeto de Lei nº 2338/23 para o uso, implementação e desenvolvimento dos sistemas de IA no Brasil, e como direitos fundamentais devem ser conjecturados na avaliação de impacto algorítmico.

Especificamente sobre mecanismos de governança relacionados a esses direitos, a análise preliminar da Autoridade Nacional de Proteção de Dados (ANPD) acerca do PL nº 2338/2023 destaca o Relatório de Impacto à Proteção de Dados (RIPD), exigido pela Lei Geral de Proteção de Dados Pessoais (LGPD), em vigência no país desde 2020, como um ponto de interação com a avaliação de impacto algorítmico (Brasil, 2023a).

Conquanto a avaliação de impacto, ante a análise da ANPD, trata-se de uma ferramenta que faculta ao agente descrever características do sistema analisado, identificar riscos e mecanismos para sua mitigação, o RIPD é a "documentação do controlador[20] que contém a descrição dos processos de tratamento de dados pessoais que

[20] A LGPD define controlador, ao artigo 5º, VI, como a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

podem gerar riscos às liberdades civis[21] e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco" (artigo 5°, XVII, LGPD).

Com relação ao conteúdo mínimo a se fazer presente no relatório de impacto, o artigo 38°, parágrafo único da LGPD, demanda a descrição dos tipos de dados coletados (se são dados pessoais sensíveis,[22] por exemplo); a metodologia utilizada para a coleta e para a garantia da segurança das informações; e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.[23]

Não obstante a diferenciação entre ambos instrumentos, o relatório produzido pela LAPIN (Lemos, 2023) questiona o porquê da demanda jurídica por uma avaliação de impacto algorítmico se já existe o RIPD, aplicável a sistemas de IA quando tratam dados pessoais regulamentado pela LGPD. A resposta, atribuída pelo relatório, concentra-se na diferença do escopo dos instrumentos.

Primeiramente porque o RIPD é uma avaliação de impacto que se dedica exclusivamente a identificar os riscos que uma atividade de tratamento de dados pode representar para um indivíduo ou um grupo de pessoas cujos dados pessoais estão sendo tratados (Lemos, 2023).

Já a avaliação de impacto algorítmico pode ser vista como um instrumento mais amplo, porquanto sua execução demanda a proteção de direitos e interesses que transcendem o tratamento de dados pessoais, incluindo a própria operacionalização do algoritmo, a estrutura da programação e a imprevisibilidade do comportamento da máquina (Lemos, 2023).

---

[21] Liberdades civis são os direitos fundamentais e garantias individuais que protegem os cidadãos contra interferências indevidas do Estado e asseguram sua autonomia na sociedade. Incluem direitos como liberdade de expressão (artigo 5, IV, IX da CRFB/88) liberdade de associação (artigo 5º, XVII a XXI da CRFB/88), liberdade religiosa (artigo 5º, VI e VIII da CRFB/88), direito à privacidade (artigo 5º, X e XII da CRFB/88), direito à propriedade (artigo 5º, XXII CRFB/88), e o devido processo legal (artigo 5º, LIV e LV da CRFB/88).

[22] Dados pessoais correspondem ao conjunto de informações que, de forma individual ou combinada, possibilitam a identificação de um indivíduo, como por exemplo o Nome, CPF, Endereço e E-mail. Por sua vez, os dados pessoais sensíveis são aqueles que, quando divulgados, podem ensejar algum tipo de discriminação, como por exemplo, informações relacionadas à saúde, raça, gênero, posicionamento político, religião, etc (Brasil, 2024).

[23] Além disso, segundo o artigo 10º § 3º da LGPD é facultado à ANPD solicitar ao controlador o relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial (Monteiro, 2024).

Para a ANPD (Brasil, 2023, p.7), "é indubitável a correlação entre as duas ferramentas, tanto no aspecto metodológico de sua elaboração, quanto no conteúdo (para os casos em que sistemas de IA tratem dados pessoais)". No exemplo citado pela autoridade nacional, é possível citar *softwares* de reconhecimento facial e aplicações de IA na área da saúde, que exigirão simultaneamente a elaboração de um RIPD e uma avaliação de impacto algorítmico (Brasil, 2023a).

Cenário análogo é vislumbrado na União Europeia. Isto porque, no Brasil, a privacidade e a proteção de dados pessoais são categorizadas como direitos fundamentais pela Constituição da República Federativa do Brasil e disciplinadas na Lei Geral de Proteção de Dados Pessoais.

Já na União Europeia, a garantia desses direitos é prevista nos artigos 7° e 8° da Carta dos Direitos Fundamentais da União Europeia (União Europeia, 2012) e são disciplinados pelo Regulamento (UE) 2016/679 denominado Regulamento Geral de Proteção de Dados (*General Data Protection Regulation* - GDPR), editado para a regulamentação do tratamento e proteção de dados pessoais no bloco europeu.

Assim, enquanto a LGPD no Brasil, elegeu a expressão "Relatório de Impacto à Proteção de Dados no Brasil", o GDPR na União Europeia, adotou o termo "avaliação de impacto sobre a proteção de dados" (União Europeia, 2018).

Apesar da finalidade de ambas as normas ser a mesma, o GDPR impõe a avaliação de impacto sobre a proteção de dados de forma mais detalhada em comparação com o RIPD da LGPD, que estabelece tão somente um conteúdo mínimo e delega à ANPD a competência para regulamentar o RIPD solicitado pela própria autoridade em face do controlador (artigo 38°, "caput" e parágrafo único da LGPD).

Esse detalhamento prossegue no artigo 35°, n.1 do GDPR. De forma similar ao Ato de IA, impõe aos responsáveis pelos sistemas de tratamento de dados que representam um risco elevado para os direitos e liberdades das pessoas singulares, a obrigatoriedade de execução da avaliação de impacto de proteção de dados em um momento *ex ante*, ou seja, antes do início do tratamento de dados.

Tal obrigatoriedade é exigida precipuamente nos casos apresentados no rol das alíneas a), b) e c) do artigo 35°, n.2, bem como para aqueles tipos de operações de

tratamento discriminados na lista pública determinada pela autoridade de controle (artigo 35°, n.4, GDPR).[24]

A avaliação de impacto sobre a proteção de dados tem seu conteúdo mínimo definido pelas alíneas a) e b), n.7 do mesmo dispositivo legal, e deve incluir uma descrição sistemática das operações de tratamento previstas e a finalidade do tratamento, incluindo, se for o caso, os interesses legítimos do responsável pelo tratamento, bem como a avaliação da necessidade das operações de tratamento em relação aos objetivos.

Além disso, as alíneas c) e d) do mesmo dispositivo legal, estabelecem a inclusão de uma avaliação e a previsão de medidas para mitigar os riscos para os direitos e liberdades dos titulares dos direitos, incluindo as garantias, medidas de segurança e procedimentos destinados a assegurar a proteção dos dados pessoais e a demonstração da conformidade com o GDPR, considerando os direitos e os legítimos interesses dos titulares dos dados e de outras pessoas em causa.

Seguindo novamente uma abordagem baseada em riscos, o GDPR em seu artigo 36°, n.1 e n.2, determina que, caso a avaliação de impacto sobre a proteção de dados indique que o tratamento representa um risco elevado, na ausência de medidas mitigadoras, o responsável pelo tratamento deve, antes de prosseguir com a atividade, realizar uma consulta prévia à autoridade de controle. Esta, por sua vez, dispõe de um prazo de oito semanas, prorrogável, a partir do recebimento do pedido, para fornecer orientações por escrito ao responsável.

Verifica-se, por fim, que além de oferecer maiores avanços no tocante à execução da avaliação de impacto sobre a proteção de dados pessoais quando comparado com a LGPD, o GDPR apresenta um ponto de interação com o AI Act, qual seja a obrigatoriedade da realização de uma avaliação de impacto. Em ambas as normativas, é imperativo ao tratamento de dados pessoais e aos sistemas de IA que oferecem um risco elevado para os direitos e liberdades das pessoas singulares, a execução das avaliações de impacto sobre a proteção de dados pessoais e de impacto aos direitos fundamentais.

[24] Igualmente, a autoridade de controle pode elaborar e tornar pública uma lista dos tipos de operações de tratamento em relação aos quais não é obrigatória uma análise de impacto sobre a proteção de dados (artigo 35°, n.5, GDPR).

É nesse sentido que o AI Act, respeitando essa intersecção, menciona o GDPR em seu artigo 27º, n. 4, e ressalta que a avaliação de impacto sobre os direitos fundamentais deve complementar a avaliação de impacto sobre a proteção de dados nos casos em que as obrigações previstas ao longo do artigo já tenham sido atendidas durante a realização desta última.

5 CONSIDERAÇÕES FINAIS

Neste artigo, propôs-se delimitar os requisitos legais do Brasil e da União Europeia no tocante à execução das avaliações de impacto dos sistemas de Inteligência Artificial considerando, nomeadamente, o Projeto de Lei nº 2338/2023; a LGPD; o AI Act e o GDPR. De forma específica, objetivou-se realizar um estudo qualitativo dessas avaliações. Cumprindo com o propósito, simetrias e assimetrias foram identificadas entre as avaliações e relatórios de impacto propostos pelos textos normativos do Brasil (LGPD e PL nº 2338/23) e da União Europeia (GDPR e AI Act).

Com relação à similaridade, avaliações de impacto algorítmico no Brasil ou de impacto aos direitos fundamentais na União Europeia, destinam-se a antecipar os potenciais danos que a atividade do sistema de IA permite oferecer a direitos fundamentais e bens protegidos pelos ordenamentos jurídicos. Sua execução é obrigatória na União Europeia (e será no Brasil, quando o PL nº 2338/23, como atualmente está redigido, for convertido em lei federal) para os sistemas de IA preliminarmente classificados como alto risco ou risco elevado.

Relatórios de impacto à proteção de dados pessoais no Brasil ou avaliações de impacto sobre a proteção de dados na União Europeia, por sua vez, consistem na análise de processos de tratamento de dados pessoais que podem resultar em riscos às liberdades civis e aos direitos fundamentais protegidos pelos ordenamentos jurídicos e, assim como as avaliações de impacto, devem incluir medidas e salvaguardas para mitigação desses riscos.

Diferentemente do GDPR que especifica casos que recaem a obrigatoriedade da realização da avaliação de impacto sobre a proteção de dados (artigo 35º, n.3 e 4), a LGPD delega à ANPD o direito de determinar do controlador a elaboração do relatório (artigo 38º).

Além disso, o presente estudo identificou o momento exigido pelos instrumentos normativos para a execução das avaliações e relatório de impacto relacionadas aos sistemas de IA de alto risco. Para aqueles agentes cujo sistema oferece um risco mínimo à pessoa humana, estão dispensados da realização de avaliação e produção de relatório de impacto de seu sistema.

Com relação ao AI Act, é determinado que as avaliações de impacto sobre os direitos fundamentais sejam elaboradas em momento anterior (*ex ante*) a implementação do sistema de IA de risco elevado no bloco europeu, facultando a atualização das informações contidas na avaliação durante o momento de utilização do sistema quando um dos elementos enumerados no artigo 27º, n.1, alterou-se ou tornou-se obsoleto.

O PL nº 2338/23, por sua vez, almeja a execução das avaliações de impacto algorítmico como processo iterativo contínuo, executado ao longo de todo o ciclo de vida dos sistemas de IA de alto risco, previamente classificados em avaliação preliminar, requeridas atualizações periódicas.

No tocante às avaliações de impacto sobre a proteção de dados, o GDPR é categórico em impor sua realização em momento anterior ao tratamento suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, sendo facultado que os responsáveis pelo tratamento realizem consultas a autoridade de controle.

A despeito das normativas delinearem quando as avaliações nos sistemas de alto risco serão realizadas, a LGPD não define um momento específico e tampouco classifica os tratamentos de dados pessoais em níveis de riscos. O relatório de impacto à proteção de dados pessoais ao ser solicitado pela ANPD deverá ser cumprido nos termos exigidos pela autoridade.

Diante do exposto, é inegável que as avaliações e produções de relatório de impacto são importantes mecanismos de governança para o uso e desenvolvimento

responsável dos sistemas de IA. Primeiramente, porque fornecem *insights* aos agentes sobre os potenciais danos do sistema. Em segundo lugar, porque em posse dessas informações, já se pode elaborar e registrar quais medidas e salvaguardas serão adotadas para impedir ou mitigar os futuros impactos em cada cenário específico.

Ainda que nem todos os riscos dos sistemas de IA possam ser previsíveis e esgotados, as avaliações de impacto inerentes aos sistemas de IA combinam diversos procedimentos e documentos que almejam tornar os impactos mensuráveis, mais controláveis e mitigáveis. Isto confere maior segurança e oferece respostas mais céleres na ocorrência de um real dano para a proteção à pessoa humana e aos direitos fundamentais.

REFERÊNCIAS

ALMADA, Marco; PETIT, Nicolas. The EU AI Act: A Medley of Product Safety and Fundamental Rights? RSC Working Paper 2023/59. **European University Institute: Robert Schuman Centre for Advanced Studies**, Fiesole, n.59, p.1-27, 2023. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4308072. Acesso em 10 mar. 2025.

ASHAR, Amar, *et. al*. Algorithmic Impact Assessments at Scale: Practitioners' Challenges and Needs. **Journal of Online Trust and Safety**, [s.l.], v. 2, n.4, p.1-27, 2024. Disponível em: https://www.tsjournal.org/index.php/jots/article/view/206. Acesso em 10 mar. 2025.

BAUCHSPIESS, Adolfo. **Introdução aos Sistemas Inteligentes**: Aplicações em Engenharia de Redes Neurais Artificiais, Lógica Fuzzy e Sistemas Neuro-Fuzzy. Brasília, DF: Engenharia Elétrica Universidade de Brasília, 2008. Disponível em: https://www.ene.unb.br/adolfo/Lectures/IC/isi.pdf. Acesso em 10 mar. 2025.

BRASIL. Autoridade Nacional de Proteção de Dados. **Análise Preliminar do Projeto de Lei (PL) nº 2338/2023**. Brasília, DF: ANPD, 6 jul. 2023a. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/analise-preliminar-do-pl-2338_2023-formatado-ascom.pdf. Acesso em: 22 fev. 2025.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, [2016]. Disponível em: https://www2.senado.leg.br/bdsf/bitstream/handle/id/518231/CF88_Livro_EC91_2016.pdf. Acesso em 20 jan. 2025.

BRASIL. Laboratório Nacional de Computação Científica. **Qual a diferença entre dados pessoais e dados sensíveis?** Brasília, DF: LNCC, 20 fev. 2024. Disponível em: https://www.gov.br/lncc/pt-br/centrais-de-conteudo/campanhas-de-conscientizacao/campanha-lgpd/2024/qual-a-diferenca-entre-dados-pessoais-e-dados-sensiveis#:~:text=Dados%20pessoais%20%C3%A9%20o%20conjunto,gerar%20algum%20tipo%20de%20discrimina%C3%A7%C3%A3o. Acesso em 10 mar. 2025.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, DF: Presidência da República [2018]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 mar. 2025.

BRASIL. Ministério do Desenvolvimento, Indústria, Comércio e Serviços. **O que é avaliação da conformidade?** Brasília, DF: INMETRO, 2016. Disponível em: https://www.gov.br/inmetro/pt-br/acesso-a-informacao/perguntas-frequentes/avaliacao-da-conformidade/o-que-e-avaliacao-da-conformidade. Acesso em: 30 jan. 2025.

BRASIL. **Projeto de Lei (PL) nº 2338/2023**. Dispõe sobre o uso da Inteligência Artificial. Brasília, DF: Presidência da República [2023b]. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/157233. Acesso em: 22 fev. 2025.

CURY, Paula Maria Nasser. Métodos de Direito Comparado: desenvolvimento ao longo do século XX e perspectivas contemporâneas. **Revista de Estudos Constitucionais, Hermenêutica e Teoria do Direito**, [s.l.], v.6, p. 176-185. Disponível em: https://revistas.unisinos.br/index.php/RECHTD/article/view/rechtd.2014.62.06/4303. Acesso em: 25 jun. 2025.

FRANZOLIN, C. J.; MONTEIRO, G. V.; LAURENTIS, L. C. D. A (In) Existência De Um Direito À Explicação De Decisões Automatizadas. **THEMIS: Revista da Esmec**, [s.l.], v. 23, n. 1, p. 65–91, 2025. Disponível em: https://revistathemis.tjce.jus.br/THEMIS/article/view/1103. Acesso em: 10 mar. 2025.

HOSSAIN, Eklas, *et. al*. Application of Big Data and Machine Learning in Smart Grid, and Associated Security Concerns: A Review. **IEEE**, [s.l.], v. 7, p. 13960-13988, 2019. Disponível em: https://ieeexplore.ieee.org/document/8625421. Acesso em: 10 mar. 2025.

JANCZURA, Rosane. Risco ou vulnerabilidade social? **Textos & Contextos (Porto Alegre)**, [S. l.], v. 11, n. 2, p. 301–308, 2012. Disponível em: https://revistaseletronicas.pucrs.br/fass/article/view/12173. Acesso em: 10 mar. 2025.

LEMOS, Alessandra; *et. al.* **Avaliação de Impacto Algorítmico para a proteção dos direitos fundamentais**. Relatório. Brasília: Laboratório de Políticas Públicas e Internet (LAPIN), 2023. Disponível em: https://lapin.org.br/wp-content/uploads/2023/04/RelatorioAIA.pdf. Acesso em: 28 jan. 2025.

MCCARTHY, John; *et. al*. **A Proposal For The Dartmouth Summer Research Project On Artificial Intelligence,** [s.l.], p.1-13, 1955. Disponível em: http://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf. Acesso em: 23 jan. 2025.

MCCARTHY, John. What is artificial intelligence? **Stanford University**. Califórnia: Condado de Santa Clara, 2007.

METCALF, Jacob, *et. al*. Algorithmic Impact Assessments and Accountability: The Co-construction of Impacts. *In:* FAccT '21 (Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency). **Proceedings** [...]. Nova York: Association for Computing Machinery, 2021. Disponível em: https://dl.acm.org/doi/10.1145/3442188.3445935. Acesso em: 10 mar. 2025.

MONTEIRO, Giovanna Voorn. **Smart Grids e a (Im) Possibilidade de Revisão de Decisões Automatizadas**. 2024. Dissertação (Mestrado em Direito) – Faculdade de Direito, Pontifícia Universidade Católica de Campinas, Campinas, 2024. Disponível em: https://repositorio.sis.puc-campinas.edu.br/xmlui/handle/123456789/17576. Acesso em: 26 jun. 2025.

OECD. **OECD/LEGAL/0449**: Recommendation of the Council on Artificial Intelligence. Paris: OECD, 22 maio 2019. Disponível em: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449. Acesso em: 26 jan. 2025.

O'NEIL, Cathy. **Algoritmos de destruição em massa:** como o big data aumenta a desigualdade e ameaça à democracia. 1. ed. Santo André: Editora Rua do Sabão, 2020.

SETZER, Valdemar W. Data, Information, Knowledge and Competence. *In*: 3RD CONTECSI (INTERNATIONAL CONFERENCE ON INFORMATION SYSYTEMS). **Anais** [...]. São Paulo: Universidade de São Paulo, 2006. Disponível em: https://www.tecsi.org/contecsi/index.php/contecsi/3contecsi/paper/view/1995/1109. Acesso em: 23 jan. 2025.

UNESCO. **Recomendação sobre a Ética da Inteligência Artificial**. Paris: UNESCO, 23 nov. 2021. Disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000381137_por. Acesso em: 26 jan. 2025.

UNIÃO EUROPEIA. [Carta dos Direitos Fundamentais (2012)]. **Carta Dos Direitos Fundamentais da União Europeia de 2012**. Bruxelas: Parlamento, Conselho e

Comissão Europeia. Disponível em: https://www.europarl.europa.eu/charter/pdf/text_pt.pdf. Acesso em: 12 fev. 2025.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016**. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Bruxelas: Parlamento Europeu e do Conselho [2018]. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679. Acesso em: 26 jan. 2025.

UNIÃO EUROPEIA. **Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024**. Relativo à criação de regras harmonizadas em matéria de inteli-gência artificial e que altera os Regulamentos (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e as Diretivas 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regulamento da Inteligência Artificial). Bruxelas: Parla-mento Europeu e do Conselho [2024]. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L_202401689. Acesso em: 26 jan. 2025.

UNIÃO EUROPEIA. **Verificador de conformidade com o Ato de IA da UE**. Bruxelas: EU Artificial Intelligence Act and Future of Life Institute (FLI), 2024. Disponível em:https://artificialintelligenceact.eu/pt/assessment/verificador-de-conformidade-com-a-lei-da-ue/. Acesso em: 1 fev. 2025.

WACHTER, Sandra; MITTELSTADT, Brent; RUSSELL, Chris. Bias Preservation in Machine Learning: The Legality of Fairness Metrics Under EU Non-Discrimination Law. **West Virginia Law Review**, Morgantown, v.123, n. 3, p.1-51, 2021. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3792772. Acesso em 10 mar. 2025.

WANG, Chenyue, et. al. The artificial intelligence divide: Who is the most vulnerable? **New Media & Society,** [s.l.], v.0, n.0, [s.p.], 2024. Disponível em: https://journals.sagepub.com/doi/epub/10.1177/14614448241232345. Acesso em 10 mar. 2025.

WATKINS, Elizabeth Anne, *et. al*. Governing Algorithmic Systems with Impact Assessments: Six Observations. *In*: AIES '21: Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society. **Proceedings** [...]. Nova York: Association for Computing Machinery, 2021. Disponível: https://dl.acm.org/doi/10.1145/3461702.3462580. Acesso em 10 mar. 2025.

WORLD ECONOMIC FORUM. **Global Risks Report 2024**. Disponível em: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf. Acesso em 26 jan. 2025.

ZWEIGERT, Konrad; KÖTZ, Hein. **Einführung in die Rechtsvergleichung auf dem Gebiete des Privatrechts**. 3. ed. Tübingen: Mohr Siebeck, 1996.