Direito, Processo e Cidadania
PPGD

ISSN 2764-8907

BREVE ANÁLISE COMPARATIVA ENTRE O PROJETO DE LEI N. 2.338/2023, DO BRASIL E O REGULAMENTO (UE) 2024/1689: SEMELHANÇAS E DIVERGÊNCIAS À LUZ DA CLASSIFICAÇÃO DOS RISCOS DAS ATIVIDADES A SEREM DESEMPENHADAS POR IA.

A BRIEF COMPARATIVE ANALYSIS BETWEEN BRAZILIAN BILL NO. 2,338/2023 AND REGULATION (EU) 2024/1689: SIMILARITIES AND DIFFERENCES IN LIGHT OF THE CLASSIFICATION OF RISKS OF ACTIVITIES TO BE PERFORMED BY AI.

Henrique Silviano Almeida Viana
Universidade Católica de Pernambuco, Recife, Brasil.

Stéfano Gonçalves Régis Toscano
Universidade Católica de Pernambuco, Recife, Brasil.

Como ser citado (modelo ABNT)
VIANA, Henrique Silviano Almeida; TOSCANO, Stefano Régis. BREVE ANÁLISE COMPARATIVA ENTRE O PROJETO DE LEI N. 2.338/2023, DO BRASIL E O REGULAMENTO (UE) 2024/1689: SEMELHANÇAS E DIVERGÊNCIAS À LUZ DA CLASSIFICAÇÃO DOS RISCOS DAS ATIVIDADES A SEREM DESEMPENHADAS POR IA. **Direito, Processo e Cidadania**. Recife, v. 4, n. 3, p.1-32, set./dez., 2025.

Resumo

Este artigo propõe uma análise comparativa das abordagens de classificação de risco adotadas no Regulamento (UE) 2024/1689 e no PL 2338/2023. O objetivo é identificar as semelhanças e diferenças nos critérios de classificação, nas categorias de sistemas consideradas de alto risco e nos mecanismos regulatórios preliminares previstos em ambos os textos. Busca-se, ademais, evidenciar a influência do modelo europeu no projeto legislativo brasileiro, contribuindo para a compreensão das tendências regulatórias globais e dos desafios específicos na implementação de um arcabouço legal para a IA no contexto brasileiro.

Palavras-chaves: Inteligência Artificial; Brasil; Análise comparativa.

Abstract

This article proposes a comparative analysis of the risk classification approaches adopted in Regulation (EU) 2024/1689 and Bill 2338/2023. The objective is to identify the similarities and differences in the classification criteria, the categories of systems considered high-risk, and the preliminary regulatory mechanisms foreseen in both texts. Furthermore, it seeks to highlight the influence of the European model on the Brazilian legislative project, contributing to the understanding of global regulatory trends and the specific challenges in implementing a legal framework for AI in the Brazilian context.

Keywords: Artificial Intelligence; Brazil; Comparative Analysis.

Introdução

A rápida evolução e a crescente aplicação da Inteligência Artificial (IA) em diversas esferas da vida têm gerado impactos significativos, desde a otimização de processos até profundas transformações sociais e econômicas. Paralelamente a este avanço, emerge a necessidade premente de quadros regulatórios que, prevendo os potenciais riscos associados ao desenvolvimento e utilização da IA, possam salvaguardar o ordenamento jurídico e a sociedade, preservando a saúde, a segurança, os direitos fundamentais e a estabilidade democrática.

Diante deste cenário global, a União Europeia estabeleceu um marco regulatório pioneiro com a aprovação do Regulamento (UE) 2024/1689, que adota uma abordagem baseada no risco para regular os sistemas de IA. Em consonância com esta tendência internacional e buscando estabelecer segurança jurídica e orientações éticas, o Brasil tem discutido propostas legislativas, como o Projeto de Lei (PL) 2338/2023, que igualmente adota uma classificação de riscos para os sistemas de IA.

Ambas compartilham a premissa de que a intensidade da regulação deve ser proporcional ao potencial dano que um sistema de IA pode causar, vedando a utilização pública de sistemas danosos à pessoa ou que ameacem a sociedade e colocando os sistemas de "alto risco" sob escrutínio mais rigoroso. Contudo, a forma como estes riscos são definidos, classificados e geridos apresenta particularidades em cada diploma. Além disso, dado o carácter mais avançado da discussão regulatória na UE, é pertinente investigar em que medida o projeto brasileiro se inspira ou replica conceitos e estruturas do regulamento europeu no que tange à classificação de risco e às obrigações associadas.

Este artigo propõe uma análise comparativa das abordagens de classificação de risco adotadas no Regulamento (UE) 2024/1689 e no PL 2338/2023. O objetivo é identificar as semelhanças e diferenças nos critérios de classificação, nas categorias de sistemas consideradas de alto risco e nos mecanismos regulatórios preliminares previstos em ambos os textos. Busca-se, ademais, evidenciar a influência do modelo europeu no projeto legislativo brasileiro, contribuindo para a compreensão das tendências regulatórias globais e dos desafios específicos na implementação de um arcabouço legal para a IA no contexto brasileiro.

Antes do início da análise proposta, cabe neste ponto considerar que é possível encontrar uma grande quantidade de trabalhos científicos pertencentes às mais diversas áreas, que conferem significado ao termo "risco", geralmente vinculado a conotações negativas. Nesse sentido, cumpre explicar que risco remete a algo que pode estar latente, em estado potencial ou virtual, portanto, que pode ou não vir a ocorrer. O risco não se opõe ao real, mas ao atual, ao que está acontecendo ou ao que pode acontecer a qualquer momento mediante a apresentação de prévios sinais. Contudo, um outro termo permite compreender tal passagem da potência ao ato.

Denomina-se de "perigo" (efetivo) à situação, ou condição limiar em que o risco se manifesta de modo perceptível e, por sua vez, tal contexto marca a passagem possível para o acionamento ou advento de um estado de crise, ou seja, da manifestação ou realização plena do risco. Contudo, para que o perigo possa ser caracterizado do modo acima é necessário que ao que se chama um tanto vagamente de situação ou condição seja acrescentado um componente adicional: o elemento subjetivo, relativo a quem sofre ou é colocado em perigo.

Tal é o sentido de vulnerabilidade que se refere à presença de seres humanos suscetíveis de interpretar a exposição (de si mesmos ou de outras pessoas) ao risco e, a depender do curso dos fatos, de perceber que se encontram expostos ao perigo.

As noções gerais acima configuram a base de alguns dos conceitos que permitiram a elaboração - atribuída à Lucien Faugères - de uma Teoria dos Riscos que veio a influenciar inúmeras pesquisas. O aprofundamento e maior detalhamento desses conceitos pode ser obtido por meio da leitura de autores como A. Betâmio de Almeida, George-Yves Kevern e Luciano Lourenço em quem nos apoiamos para elaborar a síntese das noções acima (ver referências).

2. Da Máquina Universal à Sociedade Algorítmica: A Necessidade de Regular a Inteligência Artificial

O Século XX viu nascer e se desenvolver o estudo da computação: a construção e programação de máquinas que pudessem ajudar as pessoas na conclusão de tarefas com maior nível de complexidade. Decerto, as primeiras máquinas, dada sua rudimentariedade, serviram muito mais para comprovar a viabilidade da tecnologia que para qualquer outra coisa.

Segundo PIMENTEL (2023, p. 52), o computador é modernamente definido de acordo com a compreensão de uma máquina eletrônica composta de elementos físicos e lógicos, capaz de efetuar, em linguagem natural, uma notável multiplicidade de áreas segundo os pressupostos de velocidade e precisão operacional. Se compõe de três elementos básicos: o hardware, que são os elementos físicos; o software, composto da parte lógica que possibilita

a execução das tarefas e o firmware, que proporciona uma espécie de "simbiose" entre os elementos indicados acima.

O mesmo autor também distingue a existência de sete gerações de computadores desde a instauração do que chamou de "Era Tecnológica": mal se contam 80 anos entre a primeira geração (iniciada nos primórdios da década de 40 do século passado e se encerrando por volta de 1952, caracterizada pelo hardware se compunha de válvulas à vácuo e com aplicação no campo militar), até a última, com computação quântica e não limitada aos bits clássicos, prevalente no campo desde o início da era digital.

Nesta toada, é impossível deixar de mencionar Alan Turing, cuja principal contribuição histórica, sem dúvida, foi decifrar a encriptador "Enigma", utilizado pelos nazistas para transmissão de informações vitais, como a rota e localização de submarinos durante a Segunda Guerra Mundial. A descoberta, portanto, permitiu a redução das baixas das forças aliadas, já que os comboios de navios sabiam a rota das embarcações da Marinha Alemã que faziam a patrulha das rotas entre a América e Europa.

Com relação à matéria ora em análise, é imprescindível mencionar que, em meados do século XX, Turing, considerado um dos pais da computação moderna, indagou se "as máquinas podem pensar?" Seu trabalho teórico engloba tanto a "máquina universal" (a Máquina de Turing) quanto uma proposta de "Jogo da Imitação" (o Teste de Turing), que não apenas estabeleceram os fundamentos da ciência da computação, mas também inauguraram o campo da inteligência artificial (IA), vislumbrando um futuro em que sistemas não-biológicos poderiam exibir comportamentos indistinguíveis dos humanos em certas tarefas.

> Em 1950, o cientista de computação britânico Alan Turing tentou responder o questionamento sobre a possibilidade de computadores corretamente programados serem considerados como entidades inteligentes que pensam com seu famoso trabalho "A Computação das Máquinas e a Inteligência", publicada pelo periódico "Mind". Ele sugeriu que se um computador se comporte da mesma forma que um humano, nós podemos considerá-lo inteligente, apresentando-se, então um teste especial para avaliar a inteligência de qualquer máquina. Imagine que tanto um computador quanto um ser humano respondem um teste datilografado por juízes que não conseguem ver quem ou o que está respondendo. Se os Juízes não conseguem

> distinguir a resposta do computador do da pessoa após análise das respostas textuais, então o computador foi aprovado numa versão comum do que se refere hoje como "Teste de Turing"[1].

O ambiente atual se encontra totalmente diferente da realidade do matemático britânico. Décadas após as contribuições pioneiras de Turing, o cenário tecnológico testemunha uma aceleração exponencial. As máquinas não apenas executam cada vez mais tarefas cujo monopólio humano se acreditava absoluto - no sentido proposto por ele - mas o fazem em uma escala e com uma complexidade que extrapolam muitas das crenças de sua época.

A sociedade atual se pauta cada vez mais por padrões algorítmicos, onde sistemas de IA são capazes de gerar textos coerentes e criativos até algoritmos que influenciam decisões em áreas críticas como saúde, crédito, emprego e segurança pública, tornaram-se onipresentes. No mais, o atual estado de arte das inteligências artificiais pode ser utilizado tanto para o bem quanto em detrimento de pessoas individualmente ou da própria civilização, comprovando-se, por exemplo, a exploração da tecnologia para tentar aplicar golpes financeiros e até mesmo influenciar resultados de eleições.

A capacidade desses sistemas de aprender, adaptar-se, gerar conteúdo sintético realista (como os *deepfakes*) e operar com graus crescentes de autonomia representa, por um lado, a concretização de parte da visão de Turing e, por outro, a emergência de desafios sociais, éticos e jurídicos de magnitude inédita.

> *Nunca na história permitimos que uma máquina decidisse autonomamente quem deveria viver e quem deveria morrer... Estamos prestes a cruzar essa ponte a qualquer momento*[2].

Questões como o potencial para manipulação comportamental, a exacerbação de vieses e discriminação algorítmica, a opacidade de sistemas complexos ("caixas-pretas"), os riscos à segurança e à privacidade, o impacto sobre o mercado de trabalho, a disseminação de desinformação e as ameaças aos processos democráticos e ao próprio Estado de direito deixaram de ser meras especulações teóricas para se tornarem preocupações concretas e

[1] PICKOVER, Clifford A. **Artificial Intelligence**: An Illustrated History: From Medieval Robots to Neural Networks. New York: Sterling Publishing, 2019. pag. 83

[2] AWAD, E. et al. The moral machine experiment. *Nature*, v. 563, p. 59-78, 2018. *apud* EYSENCK, Michael W.; EYSENCK, Christine. **AI vs Humans**. London: Routledge, 2022. p. 184.

urgentes. A capacidade transformadora da IA, portanto, exige uma resposta social e jurídica à altura, que possa orientar seu desenvolvimento e uso.

> *Nesse sentido, os sistemas de IA são expressões de poder que emergem de forças econômicas e políticas mais amplas, criados para aumentar os lucros e centralizar o controle para aqueles que os manejam*[3].

Assim, surgem esforços legislativos globais para estabelecer marcos regulatórios para a inteligência artificial. Essas iniciativas buscam encontrar um equilíbrio delicado: como fomentar a inovação e colher os inegáveis benefícios que a IA pode trazer, ao mesmo tempo em que se mitigam os riscos da utilização nefasta da tecnologia, buscando o desenvolvimento e aplicação ocorram de forma alinhada à segurança das instituições e dos cidadãos, e com respeito ao ordenamento jurídico?

Duas iniciativas proeminentes nesse esforço regulatório são o Regulamento (UE) 2024/1689 da União Europeia, já em vigor, e o Projeto de Lei nº 2338/2023, em avançada tramitação no Congresso Nacional brasileiro. Ambos os textos, embora com abordagens e estágios de desenvolvimento distintos, partem da premissa de que a IA não pode evoluir em um vácuo normativo e compartilham o objetivo fundamental de criar regras para os desenvolvedores, fornecedores e utilizadores de sistemas de IA visando garantir que esta poderosa tecnologia sirva ao bem-estar humano e respeite os pilares da sociedade democrática.

Inegavelmente, o projeto de lei brasileiro está revestido de grande relevância, já que, quando entrar em vigor, pautará o desenvolvimento da Inteligência Artificial em solo pátrio. É de se lembrar, inclusive, que o atual Governo Federal Brasileiro busca a instalação nacional de *data centers* - indispensáveis para o desenvolvimento e utilização de inteligências artificiais - de grandes empresas plurinacionais, entre elas a NVIDIA, grande fabricante de semicondutores[4]

Nesta senda, a análise da regulamentação europeia do tema apresenta inegável possibilidade de comparação com o projeto brasileiro. A uma, pois sua aprovação pelo

---

[3] CRAWFORD, Kate. **Atlas of AI**: Power, Politics, and the Planetary Costs of Artificial Intelligence. New Haven: Yale University Press, 2021. p. 211.

[4] https://www.uol.com.br/tilt/noticias/redacao/2025/05/05/o-plano-de-r-2-tri-para-data-centers-que-haddad-mostrara-a-amazon-e-nvidia.htm acesso em 27.05.2025

Parlamento europeu ocorreu recentemente, em 2024. A duas, pois, historicamente, o direito em vigor na Europa costuma inspirar as iniciativas brasileiras, desde a Independência. Por tais razões, a prévia análise do Regulamento (UE) 2024/1689 se fará a seguir.

3. A Estrutura do Regulamento (UE) 2024/1689: Análise dos Considerandos que tratam da análise de risco do uso da IA na União Europeia

Em uma análise prefacial, se verifica que o Regulamento, assim como outras peças de legislação europeia, se compõem dos Artigos propriamente ditos e dos Considerandos. Estes, também referidos na literatura jurídica em inglês como "recitals", constituem a parte preambular que antecede o articulado (a parte dispositiva) nos atos jurídicos derivados da União Europeia, como regulamentos e diretivas.

A sua inclusão não é meramente estilística[5], mas uma exigência de explicitação do dever de fundamentação das instituições. Conforme destacado no Guia Prático Comum do Parlamento Europeu, do Conselho e da Comissão.

Após a explicação acima, observa-se que os Considerandos do Regulamento da Inteligência Artificial (IA) da UE tem por objetivo estabelecer os objetivos e os princípios que guiam as disposições normativas. A análise de todos os 180 Considerandos é inviável ao se considerar o escopo do presente trabalho.

Contudo, é necessário destacar que os Considerandos 1-11 pautam ser o objetivo principal da norma melhorar o funcionamento do mercado interno, promovendo a adoção de uma IA centrada no ser humano e confiável, assegurando um alto nível de proteção da saúde, segurança e direitos fundamentais (incluindo democracia, Estado de direito e proteção ambiental).

Outrossim, os mesmos itens destacam a necessidade de assegurar, no âmbito da União Europeia, do desenvolvimento de tecnologias baseadas em inteligência artificial, em respeito do objetivo dos mesmos países integrantes de fomentar o apoio à inovação tecnológica.

[5] artigo 296.º do Tratado sobre o Funcionamento da União Europeia (TFUE). Este artigo determina que todos os atos jurídicos europeus devem ser "fundamentados" e "façam referência às propostas, iniciativas, recomendações, pedidos ou pareceres previstos pelos Tratados"

Nesta toada, a adoção de um regime jurídico uniforme, que evite a fragmentação do mercado interno ajuda a assegurar a livre circulação de bens e serviços baseados em IA.

> (...) a efetividade dessa regulação está condicionada à sua adoção em escala global. A ausência de uma regulamentação harmonizada a nível mundial pode, de fato, resultar em uma competição desleal entre regiões que adotam padrões rigorosos e aquelas que operam sem restrições similares. Isso cria um cenário em que produtos e serviços estrangeiros não regulamentados têm vantagens competitivas, especialmente em áreas sensíveis como a medicina, onde a inovação tecnológica é crucial[6].

Os Considerandos também estipulam as Práticas de IA Proibidas (28-45), por desrespeitarem valores da UE e direitos fundamentais, a exemplo de IAs que usem técnicas manipuladoras, subliminares ou enganadoras ou que explorem vulnerabilidades (idade, deficiência, situação socioeconómica), que impeçam os membros destes grupos de tomar decisões fundamentadas. Também foi vedada a utilização de inteligência artificial para avaliação ou classificação geral de pessoas com base em comportamento social ou características pessoais/personalidade, quanto aos riscos de prática de infração penal ou outros casos de tratamento prejudicial/desfavorável em contextos sociais, e a identificação biométrica remota em tempo real para fins policiais, exceto em situações exaustivas previstas na regulamentação. Destaca-se, ainda, vedação ao recolhimento aleatório de imagens faciais ou reconhecimento de emoções no ambiente de trabalho ou instituição de ensino.

Para os objetivos deste trabalho, os Considerandos 48 a 63 são particularmente elucidativos, pois se dedicam a explicar e justificar os critérios e as razões para a classificação de determinados sistemas de IA como de alto risco, com especial atenção àqueles que podem impactar a saúde, a segurança e, crucialmente para a presente análise, os direitos fundamentais, incluindo aqueles exercidos no âmbito da atividade jurisdicional. O legislador europeu inicia a justificação da categoria de alto risco enfatizando a proteção dos direitos fundamentais como um critério primordial.

[6] MORAES, Alexandre Rocha Almeida de; LISBOA, Andressa Felix. Regulamentação da Inteligência Artificial na União Europeia: estrutura ética, classificação de riscos e possíveis reflexos na medicina. **UNISANTA Law and Social Science**, Vol. 13, N. 2 (jul./dez. 2024), p. 28.

O Considerando 48 estabelece que a "*dimensão das repercussões negativas causadas pelo sistema de IA nos direitos fundamentais protegidos pela Carta é particularmente importante quando se classifica um sistema de IA como sendo de risco elevado*". São elencados direitos cruciais, como o direito à dignidade do ser humano, o respeito da vida privada e familiar, a proteção de dados pessoais, o direito à não discriminação, e o "*direito à ação e a um tribunal imparcial, o direito à defesa e a presunção de inocência, e o direito a uma boa administração*".

Já o Considerando 53 introduz uma nuance crucial: mesmo que um sistema de IA se enquadre nos domínios listados no Anexo III (como a administração da justiça), ele pode *não* ser considerado de alto risco se "não representar um risco significativo de prejuízo para os interesses jurídicos protegidos nesses domínios por não influenciarem significativamente a tomada de decisões ou não prejudicarem substancialmente esses interesses".

Há condições para essa exceção: se o sistema se destina a (a) desempenhar uma tarefa processual restrita (ex: transformar dados não estruturados em estruturados), (b) melhorar o resultado de uma atividade humana previamente concluída, (c) detectar padrões de tomada de decisão ou desvios sem substituir ou influenciar uma avaliação humana previamente concluída sem revisão adequada, ou (d) executar uma tarefa que é apenas preparatória para uma avaliação relevante.

Contudo, este mesmo considerando ressalva que, se o sistema de IA implicar a "definição de perfis", ele deverá "ser sempre considerados de risco elevado". Essa distinção é vital, pois permite o uso de ferramentas de IA mais simples e auxiliares no sistema de justiça sem o ônus completo dos requisitos de alto risco, desde que seu impacto decisório e potencial de dano sejam efetivamente mínimos e não envolvam definição de perfis.

Para a atividade jurisdicional e o sistema de justiça em sentido amplo, destacam-se os Considerando 59, 60 e 63. O 59 é de indispensável análise, pois reconhece o "grau substancial de desequilíbrio de poder" e os riscos de "vigilância, detenção ou privação da liberdade" e outras "repercussões negativas nos direitos fundamentais garantidos pela Carta" quando a IA é usada por autoridades policiais.

Justifica a classificação de alto risco para IA usada para avaliar risco de vitimização, polígrafos, avaliar a fiabilidade de provas, avaliar risco de cometimento de infrações (não apenas com base em perfis) e para definição de perfis em investigações criminais. A preocupação com o impacto no "direito à ação e a um tribunal imparcial, o direito à defesa e a presunção de inocência" é explícita.

O Considerando 60 afeta a administração da Justiça para pessoas em posição de vulnerabilidade, por tratar de sistemas de IA que avaliam riscos de entrada, auxiliar na análise de pedidos de asilo/visto, ou identificar pessoas nesses contextos é classificada como de alto risco devido à importância da "exatidão, a natureza não discriminatória e a transparência" para garantir o respeito aos direitos fundamentais.

Na mesma situação está o Considerando 61, que trata mais diretamente sobre a utilização da IA na atividade jurisdicional. Nesse caso, se justifica a classificação de alto risco para "sistemas de IA concebidos para serem utilizados por uma autoridade judiciária ou para, em seu nome, auxiliar autoridades judiciárias na investigação e interpretação de factos e do direito e na aplicação da lei a um conjunto específico de factos" ou em resolução alternativa de litígios com efeitos jurídicos.

A razão é o "impacto potencialmente significativo na democracia, no Estado de direito e nas liberdades individuais, bem como no direito à ação e a um tribunal imparcial". Crucialmente, o considerando afirma que "A utilização de ferramentas de IA pode auxiliar o poder de tomada de decisão dos magistrados ou da independência judicial, mas não o deverá substituir, a decisão final tem de continuar a ser uma atividade humana" e exclui sistemas para "atividades administrativas puramente auxiliares que não afetam a administração efetiva da justiça em casos individuais".

Finalmente, o Considerando 63 serve como uma ressalva importante: a classificação de um sistema de IA como sendo de alto risco por força deste Regulamento "não deverá ser interpretada como uma indicação de que a utilização do sistema é lícita ao abrigo de outros atos do direito da União ou ao abrigo do direito nacional compatível com o direito da União". Ele reitera que o Regulamento não constitui, por si só, uma base jurídica para o tratamento de dados pessoais, salvo disposição específica.

3.1. A Visão dos Considerandos sobre Risco Mínimo e Transparência Específica

Os Considerandos do Regulamento (UE) 2024/1689, além de fundamentarem as categorias de práticas proibidas e de sistemas de alto risco, também delineiam o tratamento para sistemas de IA que apresentam "risco mínimo" e aqueles que, mesmo não sendo de alto risco, demandam "obrigações de transparência específicas". Para sistemas de IA classificados como de risco mínimo, o Regulamento não estabelece requisitos obrigatórios, visando preservar o espaço para inovação.

O Considerando 165 destaca que o desenvolvimento de IA que não seja de alto risco pode fomentar uma IA confiável na União. Para tanto, incentiva os fornecedores desses sistemas a criarem, voluntariamente, "códigos de conduta" que podem adaptar alguns requisitos dos sistemas de alto risco ou aplicar elementos das Orientações Éticas da UE, como sustentabilidade e design inclusivo.

3.2. Obrigações de Transparência para Riscos Específicos

Certas aplicações de IA, independentemente de sua classificação de risco principal, podem gerar riscos específicos de engano, manipulação ou falta de clareza para o utilizador. Os Considerandos justificam, para esses casos, a imposição de obrigações de transparência.

O Considerando 26 já indica a intenção de "estabelecer obrigações de transparência para determinados sistemas de IA". Já o Considerando 132 especifica que sistemas desenhados para interagir com pessoas ou criar conteúdo podem apresentar "riscos específicos de usurpação de identidade ou dissimulação". Por isso, as pessoas devem ser informadas quando interagem com IA (a menos que óbvio) e quando expostas a sistemas de reconhecimento de emoções ou categorização biométrica (que não sejam práticas proibidas).

A questão dos conteúdos sintéticos (como *deepfakes*) é uma preocupação central. O Considerando 133 aponta para os "riscos de desinformação e manipulação em grande escala" e justifica a necessidade de os fornecedores marcarem tecnicamente tais conteúdos como gerados ou manipulados por IA. Em linha com isso, o Considerando 134 exige que os responsáveis pela implantação também revelem a natureza artificial desses conteúdos

(imagem, áudio, vídeo e, em certos contextos, texto informativo), com exceções para fins artísticos, satíricos ou quando há revisão editorial humana. Importante notar, conforme o Considerando 137, que o cumprimento dessas obrigações de transparência não atesta, por si só, a legalidade do sistema de IA sob outras legislações.

Em suma, os Considerandos do Regulamento da IA estabelecem uma abordagem diferenciada: para risco mínimo, o foco é no incentivo a boas práticas voluntárias e na aplicação da legislação geral de segurança de produtos; para riscos específicos de transparência, são impostas obrigações diretas para garantir que os indivíduos estejam cientes e protegidos contra manipulação ou engano, complementando o regime mais estrito para IA de alto risco.

Esclarecidas as disposições relevantes dos "considerandos" no que diz respeito a classificação das atividades de IA em alto risco e proibidas, a partir de agora será estudada a composição dos artigos do regulamento para, só então, poder estudar o projeto de Lei brasileiro.

4. A Concretização da Análise de Risco nos Artigos do Regulamento da IA da UE

A abordagem baseada no risco, extensamente justificada nos Considerandos do Regulamento (UE) 2024/1689, é meticulosamente traduzida em obrigações e procedimentos concretos ao longo de seus artigos. Esta seção explora como os artigos do Regulamento, após a fase introdutória dos Considerandos, definem, classificam e impõem mecanismos de análise e gestão de riscos, com ênfase particular nos sistemas de Inteligência Artificial (IA) de alto risco e nos modelos de IA de finalidade geral que apresentam risco sistêmico.

O Regulamento inicia por solidificar o conceito de risco. O Artigo 3º, ponto 2, define risco como "a combinação da probabilidade de ocorrência de danos com a gravidade desses danos", uma definição padrão que orienta toda a avaliação subsequente. Já os Artigos 6º e 7º são centrais para a classificação dos sistemas de IA, que é intrinsecamente uma forma de análise de risco preliminar.

O Artigo 6º estabelece as regras para classificar um sistema como de alto risco, seja por ser um componente de segurança de produtos listados no Anexo I ou por estar listado no

Anexo III. De forma crucial, e espelhando o Considerando (53), o Artigo 6º, n.º 3, permite que um sistema do Anexo III não seja considerado de alto risco se o fornecedor documentar que ele "não representar um risco significativo de danos para a saúde, a segurança ou os direitos fundamentais das pessoas singulares" e cumprir as condições ali especificadas, exceto se envolver definição de perfis. Isso exige uma análise de risco por parte do fornecedor para justificar a não classificação como alto risco.

Por sua vez, o Artigo 7º habilita a Comissão a alterar o Anexo III, aditando ou modificando casos de utilização de alto risco, com base numa avaliação de se os sistemas "representam um risco de danos para a saúde e a segurança ou de repercussões negativas nos direitos fundamentais" equivalente ou superior aos já listados. O Art. 7º, n.º 2, detalha os critérios para essa avaliação, incluindo a finalidade, grau de utilização, dados tratados, autonomia, potencial de dano, vulnerabilidade das pessoas afetadas e a existência de medidas de reparação ou prevenção.

O Artigo 9º é o pilar da gestão de riscos para sistemas de IA de alto risco, detalhando uma obrigação central para os fornecedores, de ser "criado, implantado, documentado e mantido um sistema de gestão de riscos" (n.1), descrito tal sistema como um "processo iterativo contínuo, planeado e executado ao longo de todo o ciclo de vida de um sistema de IA de risco elevado".

Este processo, conforme detalhado nas alíneas (a) a (d), inclui a identificação e análise dos riscos conhecidos e razoavelmente previsíveis para a saúde, segurança ou direitos fundamentais no uso previsto, a estimativa e avaliação dos riscos que podem surgir no uso previsto e em condições de utilização indevida razoavelmente previsível, a avaliação de outros riscos com base em dados do acompanhamento pós-comercialização Art. 72 e a adoção de medidas de gestão de riscos adequadas.

Esses passos ecoam o Considerando 65, que também descreve um processo de gestão de riscos, abrangendo riscos de uso previsto e indevido razoavelmente previsível. Também é espelhada no Considerando 65 a hierarquia de medidas que tornem o risco residual aceitável: eliminação ou redução por design, adoção de medidas de atenuação e controle, e prestação de informações (inclusive formação aos utilizadores).

Por fim, os itens 6 a 8 do Art. 9º exigem a testagem dos sistemas de IA de alto risco para identificar as medidas de gestão de riscos mais adequadas e garantir que funcionem como pretendido, antes da sua colocação no mercado.

Ainda, o Art. 13 exige que o desenvolvimento de sistemas de IA de risco elevado assegurem um funcionamento "suficientemente transparente" para que os usuários responsáveis pela implantação interpretem os resultados de forma adequada. Chama também a atenção, no item 3 b iii que "qualquer circunstância conhecida ou previsível, relacionada com a utilização do sistema de IA de risco elevado de acordo com a sua finalidade prevista ou em condições de utilização indevida razoavelmente previsível, que possa causar os riscos a que se refere o artigo 9.o , n.o 2, para a saúde e a segurança ou para os direitos fundamentais" deve ser incluído nas instruções de utilização da IA, alinhando-se com os Considerandos 65 e 72 sobre a comunicação de riscos.

Também de suma importância - especialmente para os operadores do Direito, à luz da Resolução CNJ n. 615/2025 é o Art. 14, que exige ferramentas de interface homem-máquina apropriadas, que permitam supervisão pessoal durante periodo de utilização da IA. O objetivo da medida é "procurar prevenir ou minimizar riscos para saúde, segurança ou direitos fundamentais", que possam ocorrer com o uso de um sistema de IA de risco elevado é utilizado, tanto quando o uso for conforme com a finalidade prevista ou mesmo em condições de uso indevido.

Do Artigo 15, se extrai a necessidade de os sistemas sejam resistentes a erros, falhas e tentativas de exploração de vulnerabilidades, inclusive com desenvolvimento de parâmetros de referência e metodologia de medição. Ademais, segundo o item 4 do mesmo artigo:

> Os sistemas de IA de risco elevado que continuam a aprender após serem colocados no mercado ou colocados em serviço são desenvolvidos de forma a eliminar ou reduzir, tanto quanto possível, o risco de resultados possivelmente enviesados que influenciem os dados de entrada de futuras operações (circuitos de realimentação), bem como a assegurar que esses resultados

> possivelmente enviesados sejam objeto de medidas de atenuação adequadas[7].

Aqui se percebe que o legislador europeu se preocupou em assegurar a redução de vieses na IA, através do processo contínuo de alimentação de informação para IAs de alto risco, tanto através do controle dos dados informados quanto de medidas de atenuação.

5. Responsabilidades na Cadeia de Valor e Deveres dos Utilizadores de IA de Alto Risco no Regulamento Europeu (Artigos 22 a 27)

A eficácia do Regulamento (UE) 2024/1689 (Regulamento da IA) na mitigação dos riscos associados aos sistemas de Inteligência Artificial (IA) de alto risco não depende apenas dos requisitos técnicos impostos aos sistemas em si, mas fundamentalmente da clara delineação das responsabilidades dos diversos atores envolvidos em sua disponibilização e utilização. Os Artigos 22 a 27 do referido diploma são cruciais nesse sentido, pois estabelecem atribuições para os diversos responsáveis desde o ponto de entrada de sistemas de IA de alto risco no mercado da União, passando pela cadeia de distribuição, até o responsável pela sua implantação efetiva, culminando na exigência de uma avaliação proativa dos impactos sobre os direitos fundamentais. Esta seção analisa detalhadamente o escopo e as implicações dessas disposições.

5.1 O Mandatário como Ponto de Contato e Responsabilidade na UE (Artigo 22º)

Para assegurar a aplicação e a fiscalização do Regulamento sobre sistemas de IA de alto risco cujos prestadores (fornecedores) não estão estabelecidos na União Europeia, o Artigo 22º impõe a designação de um mandatário estabelecido na UE. Este mandatário, atuando sob mandato escrito, torna-se um elo crucial. Suas funções primordiais incluem verificar a elaboração da declaração UE de conformidade e da documentação técnica pelo prestador, manter essa documentação à disposição das autoridades nacionais competentes

[7] UNIÃO EUROPEIA. Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, que estabelece regras harmonizadas em matéria de inteligência artificial e altera os Regulamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 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 (Lei da Inteligência Artificial). *Jornal Oficial da União Europeia*, Luxemburgo, L 1689, 12 jul. 2024, Art. 13.º, n.º 1.

por dez anos, e cooperar com estas autoridades, fornecendo informações e assistência para demonstrar a conformidade do sistema.

O mandatário também deve informar as autoridades caso considere que o prestador está a agir em desconformidade com o Regulamento, podendo inclusive pôr termo ao mandato. Esta figura é essencial para garantir a responsabilização e um ponto de contato efetivo dentro da jurisdição da UE.

5.2 Deveres de Verificação dos Importadores (Artigo 23º)

Os importadores, como primeiro ponto de introdução de um sistema de IA de alto risco de país terceiro no mercado da União, possuem deveres de verificação específicos sob o Artigo 23º. Antes de colocar o sistema no mercado, o importador deve assegurar que o prestador cumpriu as suas obrigações essenciais, nomeadamente: a realização do procedimento de avaliação da conformidade, a elaboração da documentação técnica, a aposição da marcação CE, a existência da declaração UE de conformidade e das instruções de utilização, e a designação de um mandatário.

Caso detecte não conformidade ou suspeite de falsificação, o importador não deve colocar o sistema no mercado e, se houver risco, deve alertar as autoridades. Adicionalmente, o importador deve indicar seus dados de contato no sistema ou embalagem e manter cópias da documentação de conformidade por dez anos.

5.3 A Diligência dos Distribuidores na Cadeia de Fornecimento (Artigo 24º)

O Artigo 24º estende a cadeia de responsabilidade aos distribuidores. Antes de disponibilizarem um sistema de IA de alto risco no mercado, devem verificar se este ostenta a marcação CE, se está acompanhado da declaração UE de conformidade e das instruções de utilização, e se o prestador e o importador (se aplicável) cumpriram os seus deveres de identificação.

Tal como o importador, o distribuidor não deve disponibilizar um sistema que considere não conforme ou que apresente risco, devendo informar o prestador ou importador. Se uma não conformidade for detectada após a disponibilização, o distribuidor

deve tomar ou assegurar medidas corretivas e informar as autoridades em caso de risco. A cooperação com as autoridades é também um dever.

5.4 Atribuição de Responsabilidades em Cenários de Modificação ou *Rebranding* (Artigo 25º)

O Artigo 25º aborda a complexidade da cadeia de valor da IA, clarificando situações em que um ator (distribuidor, importador, responsável pela implantação ou outro terceiro) pode ser considerado "prestador" para efeitos do Regulamento, ficando sujeito às obrigações do Artigo 16º. Isso ocorre se este ator: (a) colocar o seu nome ou marca num sistema de IA de alto risco já existente; (b) realizar uma "modificação substancial" (que afete a conformidade ou altere a finalidade prevista) num sistema de alto risco; ou (c) modificar a finalidade de um sistema de IA (incluindo um GPAI) que não era de alto risco, de forma a torná-lo de alto risco.

Nesses casos, o prestador original cessa essa qualidade para o sistema específico, mas deve cooperar com o novo prestador, fornecendo informações e assistência. O artigo também especifica que o fabricante de um produto final que integra IA de alto risco é considerado o prestador dessa IA se a comercializar sob seu nome ou marca. Adicionalmente, prevê a necessidade de acordos escritos entre prestadores de IA de alto risco e terceiros que forneçam componentes ou ferramentas, para assegurar o cumprimento das obrigações.

5.5 Obrigações Essenciais dos Responsáveis pela Implantação (Utilizadores) (Artigo 26º)

O Artigo 26º impõe um conjunto significativo de deveres aos responsáveis pela implantação (utilizadores) de sistemas de IA de alto risco. Estes devem: utilizar os sistemas de acordo com as instruções de utilização; assegurar uma supervisão humana eficaz por pessoal competente e formado; garantir a pertinência e representatividade dos dados de entrada, se estiverem sob seu controle; monitorizar o funcionamento do sistema e comunicar riscos ou incidentes graves ao prestador e/ou autoridades; e manter os registos (logs) gerados pelo sistema. Empregadores devem informar os trabalhadores sobre o uso de IA de alto risco no local de trabalho.

Autoridades públicas que utilizam sistemas do Anexo III devem registar esse uso na base de dados da UE. O artigo também estabelece a obrigação de utilizar as informações do

prestador para realizar Avaliações de Impacto sobre a Proteção de Dados (DPIA), quando aplicável, e impõe condições específicas para o uso de identificação biométrica remota "em diferido" por autoridades policiais, incluindo a necessidade de autorização judicial ou administrativa. Finalmente, os utilizadores devem informar as pessoas singulares quando estas estão sujeitas a decisões tomadas ou auxiliadas por IA de alto risco que as afetem significativamente.

6. A Avaliação de Impacto sobre os Direitos Fundamentais como Dever do Utilizador (Artigo 27º)

Como um mecanismo proativo de proteção, o Artigo 27º introduz a obrigação de realizar uma avaliação de impacto sobre os direitos fundamentais (FRIA) antes da implementação de um sistema de IA de alto risco. Esta obrigação recai sobre responsáveis pela implantação que sejam organismos de direito público, entidades privadas que prestam serviços públicos, ou que utilizem IA para avaliação de crédito ou seguros de vida e saúde.

A FRIA deve detalhar os processos de utilização da IA, o período e frequência de uso, as categorias de pessoas afetadas, os riscos específicos de dano aos direitos fundamentais (considerando a informação do prestador), a aplicação da supervisão humana e as medidas de mitigação e recurso em caso de materialização dos riscos. Os resultados devem ser notificados à autoridade de fiscalização do mercado, e a FRIA deve complementar eventuais DPIAs já realizadas.

> A FRIA (Avaliação de Impacto nos Direitos Fundamentais) foi introduzida pelo Parlamento Europeu durante o processo legislativo da Lei da IA como uma obrigação para os implementadores de IA [AI deployers], uma categoria adicionada pelo Parlamento para preencher a lacuna entre os fornecedores de IA e os usuários finais, enfatizando o papel que os implementadores podem desempenhar ativamente no uso contextual e nas customizações dos sistemas de IA.[64] Em linha com a teoria geral do risco, o ônus da gestão do risco é, portanto, compartilhado proporcionalmente entre os fornecedores e os implementadores de IA, de acordo com o risco real introduzido na sociedade e seu respectivo poder de gerenciá-lo.[8]

[8] Alessandro Mantelero, "The Fundamental Rights Impact Assessment (FRIA) in the AI Act: Roots, legal obligations and key elements for a model template," **Computer Law & Security Review: The International Journal of Technology Law and Practice** 54 (2024): 106020, https://doi.org/10.1016/j.clsr.2024.106020, P. 07.

Ainda sobre o tema, é indispensável mencionar o Artigo 72º, que fala sobre o acompanhamento pós comercialização. Ele obriga os fornecedores a recolherem dados sobre o desempenho dos sistemas de IA de alto risco ao longo da sua vida útil para "avaliar a contínua conformidade", o que implicitamente envolve a reavaliação de riscos e a identificação de novos, como sugerido no Art. 9º, n.º 2.

Estabelecidas as bases para análise e classificação de riscos de adoção de tecnologias baseadas e, inteligência artificial, e dos responsáveis durante o processo, torna-se necessário, agora, entender de que forma o Projeto de Lei nº 2338/2023 trata a questão para, em seguida, comparar os dois textos.

7. A Estratificação de Riscos no Projeto de Lei Brasileiro sobre Inteligência Artificial (PL 2338/2023)

Inicialmente, é de se destacar que o Projeto de Lei nº 2338/2023 (conhecida popularmente como "PL da IA") também adota uma abordagem regulatória centrada no grau de risco, delineado principalmente em seu Capítulo III (Da Categorização dos Riscos, Arts. 12 a 16). Este capítulo estabelece os mecanismos para identificar o grau de risco dos sistemas de Inteligência Artificial (IA), com ênfase na definição do que constitui "risco excessivo" – resultando em proibição – e "alto risco", que acarreta um conjunto de obrigações de governança específicas.

7.1 Avaliação Preliminar e a Determinação do "Grau de Risco" (Artigo 12º)

O PL da IA incentiva, em seu Artigo 12º, que os agentes de IA realizem, antes da introdução do sistema no mercado ou de seu emprego, uma avaliação preliminar para "determinar o grau de risco do sistema". Esta autoavaliação é considerada uma medida de boa prática, podendo conferir benefícios ao agente, como prioridade em processos de avaliação de conformidade. As autoridades setoriais têm a prerrogativa de simplificar ou dispensar essa avaliação em certos casos, e a autoridade competente pode, mediante processo, determinar a reclassificação do sistema ou a necessidade de uma avaliação de impacto algorítmico mais aprofundada.

7.2 Risco Excessivo: Práticas de IA Vedadas (Artigo 13º)

Correspondendo às práticas de risco inaceitável em outras jurisdições, o Artigo 13º do PL da IA lista os sistemas cujo desenvolvimento, implementação e uso são vedados devido ao "risco excessivo" que apresentam. As proibições abrangem sistemas com o propósito de instigar ou induzir comportamento danoso à saúde, segurança ou direitos fundamentais, ou que explorem vulnerabilidades para o mesmo fim, que avaliem traços de personalidade ou comportamento passado para prever risco de cometimento de crimes ou reincidência, que possibilitem a produção ou disseminação de material de abuso ou exploração sexual infantojuvenil.

Também vedam o uso, pelo Poder Público, de sistemas para "avaliar, classificar ou ranquear as pessoas naturais, com base no seu comportamento social ou em atributos da sua personalidade, por meio de pontuação universal, para o acesso a bens e serviços e políticas públicas, de forma ilegítima ou desproporcional", criação de armas autônomas, identificação biométrica à distância, em tempo real e em espaços acessíveis ao público, excetuando-se hipóteses estritas (instrução de inquérito/processo criminal com autorização judicial prévia e motivada, busca de vítimas/desaparecidos em situações de ameaça grave, flagrante de crimes graves com comunicação judicial imediata, e recaptura de foragidos/cumprimento de mandados judiciais)

7.3 Alto Risco: Definição, Contextos de Uso e Processo Regulatório (Artigos 14º ao 16º)

O PL da IA define no Artigo 14º os sistemas de "alto risco" com base em suas finalidades e contextos de uso, considerando a probabilidade e a gravidade de impactos adversos. A lista exemplificativa inclui IA empregada em: infraestruturas críticas (como controle de trânsito e redes de abastecimento), processos seletivos decisórios em educação e emprego, acesso a serviços essenciais públicos e privados (assistência, crédito); administração da justiça (auxílio a autoridades judiciárias na investigação de fatos e aplicação da lei com risco a liberdades); veículos autônomos; saúde (auxílio a diagnósticos e procedimentos médicos); estudo analítico de crimes e perfis comportamentais; investigações administrativas para avaliar provas ou prever infrações com base em perfis; identificação biométrica para reconhecimento de emoções; e gestão de imigração e controle de fronteiras.

O parágrafo único do Art. 14º isenta dessa classificação a IA utilizada como "tecnologia intermediária que não influencie ou determine resultado ou decisão ou quando desempenha uma tarefa processual restrita".

O Artigo 15º estabelece que o Sistema Nacional de Regulação e Governança de Inteligência Artificial (SIA) regulamentará a lista de sistemas de alto risco e identificará novas hipóteses, com base em critérios como o potencial de produzir efeitos jurídicos relevantes, viés discriminatório, impacto em grupos vulneráveis, e grau de transparência e auditabilidade. No mais, o Artigo 16º detalha o processo para essa regulamentação, envolvendo participação social, análise de impacto regulatório, e a atuação coordenada entre a autoridade competente (ANPD) e as autoridades setoriais.

7.4 Abordagem para Riscos Inferiores (Moderado e Leve)

Ao passo que o Capítulo III do Projeto de Lei nº 2338/2023 dedica-se com minúcia à identificação e ao tratamento regulatório dos sistemas de Inteligência Artificial (IA) classificados como de "risco excessivo" (resultando em sua vedação) e de "alto risco" (sujeitando-os a um robusto arcabouço de governança), a abordagem para os riscos que se situariam em patamares inferiores – por vezes denominados como moderados ou leves – não se traduz na criação de categorias formais estanques com regimes de obrigações específicos e escalonados dentro deste mesmo capítulo. A menção no **Artigo 12º** à "determinação do 'grau de risco'" por meio de uma avaliação preliminar sugere, de fato, a concepção de um espectro de riscos. Contudo, o foco legislativo subsequente no Capítulo III é, inequivocamente, a distinção e o tratamento rigoroso das categorias de maior impacto potencial.

Para os sistemas de IA que não se enquadram como de risco excessivo ou alto, e que, portanto, transitariam por esses graus inferiores de risco, o PL 2338/2023 parece indicar uma estratégia regulatória que, em vez de detalhar regimes de conformidade distintos e obrigatórios para cada subnível, ancora-se na força normativa de seus preceitos mais amplos e no fomento a uma cultura de responsabilidade.

A sua governança é, assim, orientada em primeiro lugar, pela aplicação dos fundamentos da lei, conforme disposto nos Artigos 2º e 3º, que perpassa toda e qualquer

aplicação de IA, independentemente de seu risco específico. Fundamentos como a "centralidade da pessoa humana", o "respeito e promoção aos direitos humanos e aos valores democráticos", e princípios como a "não discriminação ilícita ou abusiva", a "justiça, equidade e inclusão", a "transparência e explicabilidade" e a "prevenção, precaução e mitigação de riscos e danos" servem como diretrizes interpretativas e de conduta para todos os agentes, inclusive aqueles que desenvolvem ou aplicam sistemas de IA de risco inferior. Soma-se a isso a garantia dos direitos básicos das pessoas afetadas por *qualquer* sistema de IA, conforme o Artigo 5º, que inclui o direito à informação sobre interações com IA e à não discriminação.

Também se aplicam independentemente do grau de risco da IA a transparência para funcionalidades específicas, a exemplo do Art. 19, que exige que sistemas de IA que gerem conteúdo sintético incluam um identificador para verificação de sua proveniência ou modificações.

> Que o olhar humano está na mira dos algoritmos é uma outra questão que merece ser elucidada já que interfere diretamente no funcionamento nocivo das deep fakes . Essa elucidação, tanto quanto o funcionamento do sistema perceptivo humano, também não é imediatamente evidente já que se apresenta como um paradoxo do visível e do invisível: o nosso olhar, justamente o que nos permite a visualização dos fenômenos, está sendo manipulado pelos algoritmos no plano da invisibilidade[9].

Desta forma, o PL 2338/2023, ao mesmo tempo que concentra seu poder de comando e controle nas categorias de IA de maior potencial lesivo, delineia para os demais sistemas um caminho que valoriza a internalização dos princípios éticos e jurídicos fundamentais, o empoderamento do cidadão através da transparência em usos específicos, e a construção de uma governança responsável e participativa, fomentada pela própria comunidade de desenvolvedores e aplicadores.

Opta-se, assim, por uma flexibilidade orientada por princípios e pelo estímulo à corresponsabilidade, em detrimento da criação de múltiplos escalonamentos formais de risco com regimes de conformidade distintos e obrigatórios no seu capítulo central de classificação. Essa abordagem busca, presumivelmente, não engessar a inovação em

[9] BATISTA, Anderson Röhe Fontão; SANTAELLA, Lucia. Prognósticos das deepfakes na política eleitoral. **Organicom**, São Paulo, Brasil, v. 21, n. 44, p. 187–196, 2024. DOI: 10.11606/issn.2238-2593.organicom.2024.221294. Disponível em: https://revistas.usp.br/organicom/article/view/221294., p. 192.

aplicações de menor impacto, ao mesmo tempo que assegura que o desenvolvimento e uso da IA no país permaneçam firmemente ancorados na proteção da pessoa humana e nos valores democráticos.

7.5 A Governança da Inteligência Artificial na Prática: Responsabilidades dos Aplicadores e a Avaliação de Impacto Algorítmico no PL 2338/2023

A regulamentação da Inteligência Artificial (IA) transcende a mera estipulação de requisitos técnicos para os sistemas, abarcando de forma crucial as responsabilidades dos diversos atores que interagem com essa tecnologia ao longo de seu ciclo de vida. O Projeto de Lei nº 2338/2023 (PL da IA brasileiro), em linha com tendências internacionais como o Regulamento (UE) 2024/1689 (Regulamento da IA da UE), dedica especial atenção aos deveres daqueles que efetivamente empregam ou utilizam os sistemas de IA, denominados "aplicadores". Esta seção analisa as obrigações impostas a esses agentes pelo PL brasileiro, com destaque para o setor público, e, subsequentemente, aprofunda-se na Avaliação de Impacto Algorítmico (AIA) como ferramenta central de accountability, estabelecendo um paralelo com os mecanismos previstos na legislação europeia.

8. Responsabilidades dos Aplicadores de Sistemas de IA no PL 2338/2023

O PL 2338/2023 define "aplicador", em seu Artigo 4º, inciso VII, como a "pessoa natural ou jurídica, de natureza pública ou privada, que empregue ou utilize, em seu nome ou benefício, sistema de IA inclusive configurando, mantendo ou apoiando com o fornecimento de dados para a operação e o monitoramento do sistema de IA". Aos aplicadores de sistemas de IA de alto risco, o Artigo 18, inciso I, do PL impõe um conjunto de medidas de governança e processos internos essenciais para um uso responsável e mitigador de riscos.

Essas medidas incluem manter documentação apropriada referente a todas as etapas relevantes do ciclo de vida do sistema que estão sob sua esfera de atuação, avaliação contínua e mitigação de riscos, realização de testes de confiabilidade e segurança, manter registros sobre o grau de supervisão humana que contribuiu para os resultados apresentados pelos sistemas de IA prevenção e mitigação de vieses discriminatórios e manter transparência, assegurando o direito à explicação.

8.1 Ênfase nas Obrigações do Setor Público como Aplicador

O PL 2338/2023 demonstra uma preocupação acentuada com a utilização de IA pelo poder público, estabelecendo deveres adicionais no **Artigo 23**. Ao desenvolver, contratar ou adotar sistemas de IA de alto risco, todos os entes da Administração Pública direta e indireta (incluindo, conforme §5º, órgãos dos Poderes Legislativo e Judiciário em funções administrativas e pessoas jurídicas de direito privado responsáveis pela gestão de serviços públicos) devem:

- Definir protocolos de acesso e utilização do sistema que permitam o registro de quem o utilizou, para qual situação concreta e com qual finalidade (Art. 23, I).
- Garantir, de forma facilitada e efetiva, o direito do cidadão à explicação e à revisão humana de decisões tomadas por sistemas de IA que gerem efeitos jurídicos relevantes ou que impactem significativamente seus interesses (Art. 23, II). Esta disposição reforça o direito à explicação já previsto no Artigo 6º do PL e encontra forte paralelo no Artigo 86 do Regulamento da UE, além de ressoar com as obrigações de transparência do Artigo 26, parágrafo 11, da legislação europeia.
- Publicizar em veículos de fácil acesso as avaliações preliminares dos sistemas de IA de alto risco que desenvolvem, implementam ou utilizam (Art. 23, III).

Essa ênfase na *accountability* do setor público é crucial, dado o impacto direto das decisões estatais na vida dos cidadãos e a necessidade de assegurar que o uso de IA pelo Estado esteja alinhado com os princípios democráticos e a proteção dos direitos fundamentais.

8.2. A Avaliação de Impacto Algorítmico (AIA) no PL 2338/2023: Equivalência à FRIA Europeia e Instrumento Chave de Responsabilização

Para além das obrigações operacionais e de governança contínua, o PL 2338/2023 institui a Avaliação de Impacto Algorítmico (AIA) como um mecanismo central de análise de risco e responsabilização prévia, especialmente para sistemas de IA de alto risco. Este instrumento é o equivalente funcional direto da Avaliação de Impacto sobre os Direitos Fundamentais (FRIA), estabelecida pelo Artigo 27 do Regulamento da IA da UE.

O Artigo 4º, inciso XVI, do PL define a AIA como a "análise do impacto sobre os direitos fundamentais, apresentando medidas preventivas, mitigadoras e de reversão dos impactos negativos, bem como medidas potencializadoras dos impactos positivos de um

sistema de IA". O seu propósito, portanto, alinha-se integralmente ao da FRIA europeia: uma avaliação ex ante dos riscos aos direitos fundamentais.

Conforme o Artigo 25º, caput, a AIA é uma obrigação "do desenvolvedor ou do aplicador que introduzir ou colocar sistema de IA em circulação no mercado, sempre que o sistema ou o seu uso forem de alto risco". A metodologia, segundo o §1º do mesmo artigo, deve contemplar, no mínimo, a "avaliação dos riscos e benefícios aos direitos fundamentais, medidas de atenuação e efetividade dessas medidas de gerenciamento". A autoridade competente, conforme o §5º do Artigo 25, estabelecerá critérios gerais e elementos para sua elaboração. Adicionalmente, o Artigo 23, §1º, do PL impõe especificamente que a utilização de sistemas biométricos para fins de identificação pelo poder público seja precedida de uma AIA.

A AIA deve ser realizada "em momento anterior à introdução ou à colocação em circulação no mercado" e, crucialmente, "consistirá em processo interativo contínuo, executado ao longo de todo o ciclo de vida dos sistemas de IA de alto risco, requeridas atualizações periódicas" (Artigo 26º). Esta natureza é um aspecto importante, que sublinha a necessidade de reavaliação constante dos impactos à medida que o sistema evolui ou seu contexto de uso se altera.

Buscando eficiência e sinergia, o Artigo 27º do PL permite que a AIA "poderá ser realizada em conjunto" com o Relatório de Impacto à Proteção de Dados Pessoais (RIPD) exigido pela Lei Geral de Proteção de Dados Pessoais (LGPD), uma abordagem similar à prevista no Artigo 27(4) do Regulamento da UE, que estabelece que a FRIA deve complementar a avaliação de impacto sobre a proteção de dados.

Um ponto de destaque no PL brasileiro é a determinação do Artigo 28º de que "As conclusões da avaliação de impacto algorítmico serão públicas, observados os segredos industrial e comercial, nos termos de regulamento". Esta previsão de publicidade das conclusões da AIA, embora sujeita a regulamentação e ressalvas, tem o potencial de fomentar um maior escrutínio público e controle social sobre os sistemas de IA de alto risco, indo talvez um passo além da mera notificação dos resultados da FRIA às autoridades de fiscalização, como previsto no Artigo 27(3) do diploma europeu.

Finalmente, a ênfase na responsabilização do aplicador, especialmente o público, é reforçada pela consequência estabelecida no Artigo 23, §2º: "Na impossibilidade de eliminação ou mitigação substantiva dos riscos associados ao sistema de IA identificados na avaliação de impacto algorítmico [...] sua utilização será descontinuada". Esta disposição confere um peso significativo aos resultados da AIA no setor público, condicionando a continuidade do uso da tecnologia à efetiva gestão dos seus riscos para os direitos fundamentais.

8.3 AIA, FRIA e a Responsabilidade dos Aplicadores

A Avaliação de Impacto Algorítmico, conforme proposta no PL 2338/2023, emerge como um instrumento central para a concretização de uma IA ética e responsável no Brasil. Sua funcionalidade espelha a da FRIA europeia, ao focar na análise prévia dos impactos sobre direitos fundamentais. No entanto, o PL brasileiro confere à AIA uma potencial amplitude de publicidade e estabelece consequências diretas para o setor público em caso de riscos não mitigáveis, reforçando a centralidade e a responsabilidade dos aplicadores que o utilizam em contextos de alto risco.

9. Análise Comparativa das Abordagens à Classificação e Gestão de Riscos em Inteligência Artificial: O Regulamento UE 2024/1689 e o PL 2338/2023 Brasileiro

A regulamentação da Inteligência Artificial (IA), tanto na União Europeia (UE) através do Regulamento (UE) 2024/1689 (Regulamento da IA) quanto na proposta brasileira consubstanciada no Projeto de Lei nº 2338/2023 (PL da IA), adota, como visto anteriormente, uma abordagem fundamentalmente baseada no risco, que justifica as diferentes obrigações, proibições e mecanismos de supervisão. No entanto, apesar da convergência conceitual, existem nuances significativas na forma como cada um desses marcos normativos define, categoriza e propõe a gestão dos riscos inerentes aos sistemas de IA. Esta seção propõe uma análise comparativa dessas abordagens, com foco na classificação dos riscos e nos sistemas de gestão preconizados.

9.1. Fundamentos e Definição de Risco

Ambos os diplomas partem da premissa de que nem toda aplicação de IA necessita do mesmo nível de escrutínio regulatório. A intensidade da regulação deve ser proporcional ao potencial de dano que um sistema de IA pode causar à saúde, segurança e aos direitos fundamentais.

O Regulamento da UE, em seu Artigo 3º, ponto 2, define risco como "a combinação da probabilidade de ocorrência de danos com a gravidade desses danos". Os Considerandos reforçam que essa avaliação de risco deve considerar o impacto nos direitos fundamentais como um elemento central.

Já o PL 2338/2023 brasileiro não traz uma definição isolada de "risco", apesar de o Artigo 12º prever a "avaliação preliminar" que o agente de IA pode realizar para "determinar o grau de risco do sistema". Ademais, o Artigo 3º afirma como princípio a "prevenção, precaução e mitigação de riscos e danos".

9.2. Categorização dos Níveis de Risco: Semelhanças e Divergências

Ambos os textos identificam categorias de risco que orientam a regulamentação da atividade. Num patamar proibido, os riscos inaceitáveis/excessivos estão no Artigo 5º do Regulamento da UE e no Artigo 13º do PL 2338/2023. lista práticas de IA consideradas de risco inaceitável e, portanto, proibidas. Em harmonia com os Considerandos 28-45 da legislação europeia, essas práticas incluem manipulação subliminar ou exploratória, "social scoring" por autoridades públicas, e certos usos de identificação biométrica remota em tempo real, com exceções muito estritas e condicionadas.

O Regulamento da UE (Art. 6º) classifica como de alto risco sistemas que são componentes de segurança de produtos listados no Anexo I (sob certas condições) ou sistemas autônomos listados nos domínios do Anexo III (como biometria, infraestruturas críticas, educação, emprego, serviços essenciais, aplicação da lei, gestão de migração e administração da justiça). O PL 2338/2023 (Art. 14º) também lista finalidades e contextos de uso que tornam um sistema de IA de alto risco, com muitas sobreposições com o Anexo III da

UE (infraestruturas críticas, educação, emprego, serviços essenciais, saúde, administração da justiça, identificação biométrica para reconhecimento de emoções etc.).

O parágrafo único do Art. 14º do PL, de forma análoga ao Art. 6º da UE, prevê que não se considera de alto risco IA usada como "tecnologia intermediária que não influencie ou determine resultado ou decisão ou quando desempenha uma tarefa processual restrita"

Quanto à classificação de riscos médios, inferiores ou mínimos, o Regulamento da UE não cria uma categoria formal de "risco moderado" ou "leve", mas estabelece, em seu Capítulo IV (Art. 50), "obrigações de transparência específicas" para certos sistemas que podem não ser de alto risco, mas apresentam riscos de engano ou manipulação (ex: chatbots, sistemas de reconhecimento de emoções não proibidos, *deepfakes*). Para sistemas de "risco mínimo", o Regulamento incentiva códigos de conduta voluntários (Considerando 165). Da mesma forma, conforme visto anteriormente, não há uma definição formal de categorias de "risco moderado" ou "risco leve" com regimes regulatórios distintos e escalonados nesse capítulo.

Na Lei Brasileira, os sistemas de menor risco serão implicitamente aqueles que não se enquadram nas categorias superiores. Sua regulação se daria pela aplicação dos princípios e fundamentos gerais da lei (Arts. 2º e 3º), pelos direitos básicos das pessoas afetadas (Art. 5º), por obrigações de transparência pontuais (como a do Art. 19º sobre identificação de conteúdo sintético), e pelo incentivo à adoção de códigos de boas práticas e autorregulação (Arts. 40º e 41º).

Quanto à avaliação e gestão de riscos para estes sistemas, ao menos a nível programático, ambos os diplomas exigem mecanismos robustos para a gestão contínua dos riscos em sistemas de alto risco. O Regulamento da UE, no Artigo 9º, detalha um sistema de gestão de riscos que deve ser implementado pelo fornecedor ao longo de todo o ciclo de vida da IA de alto risco. Inclui identificação, análise, estimativa, avaliação de riscos (uso previsto e indevido razoavelmente previsível), adoção de medidas de mitigação hierarquizadas e testagem.

Por sua vez, o PL 2338/2023, no Artigo 18º estabelece as "medidas de governança" para desenvolvedores e aplicadores de IA de alto risco. Para os desenvolvedores (Art. 18, II),

isso inclui manter registro das medidas de governança, usar ferramentas de registro da operação para avaliação de acurácia e robustez, realizar testes de segurança, e adotar medidas para mitigar vieses discriminatórios, sendo este último item uma inovação em relação à legislação europeia. Avaliação de Impacto sobre Direitos Fundamentais (Utilizadores/Aplicadores):

Os dois textos legais exigem que os responsáveis pela implantação de sistemas de IA realizem um análise do impacto destes nos direitos fundamentais: a FRIA na UE (Art. 27), a ser realizado por organismos públicos e privados que exerçam atividades essenciais e AIA (Avaliação de Impacto Algorítmico) no Projeto de Lei Brasileiro (Arts. 25 a 28)., para desenvolvedor ou aplicador de IA de alto risco. Funcionalmente, ambos os mecanismos se equivalem, pois focam na análise prévia e na necessidade da adoção de medidas de mitigação.

Quanto à possibilidade de atualização regulatória baseada em riscos das IA, percebe-se uma diferença marcante entre as duas legislações. Isso porque o projeto brasileiro institui, através do seu Art. 4º, IX, uma autoridade competente cuja função é coordenar o Sistema Nacional de Regulação e Governança de Inteligência Artificial (SIA), cujo objetivo, nos termos do inciso X do mesmo diploma legal, é "promover e garantir a cooperação e harmonização com as demais autoridades setoriais e entes reguladores, sem vínculo de subordinação hierárquica entre eles e outros sistemas nacionais para a plena implementação e fiscalização do cumprimento desta lei em todo o território nacional, com segurança jurídica".

O Artigo 15 detalha a organização e atribuições do SIA, inclusive prevendo a possibilidade de novas hipóteses de aplicação da classificação de alto risco a sistemas de IA, "levando em consideração a probabilidade e gravidade dos impactos adversos sobre pessoas ou grupos afetados". Dessa forma, o projeto de lei brasileiro prevê a possibilidade de modificação do rol de atividades de alto risco se desempenhadas por IA, no seio de um sistema gerido por Autoridade Central de âmbito federal.

Por outro lado, o Artigo 7º do Regulamento 2024 1689 da União Europeia atribui à Comissão Europeia a possibilidade de alterar a lista de alto risco do Anexo III do mesmo diploma legal, com base em novos riscos identificados, inclusive com base no

acompanhamento pós-comercialização (Art. 72º), que também alimenta a reavaliação de riscos.

A Comissão Europeia, como é consabido, é o próprio órgão executivo da UE, assumindo inclusive a função de negociar acordos internacionais em nome do bloco, organizar o orçamento, dentre outras. Assim, se percebe que, no âmbito da União Europeia, o próprio Poder Executivo detém o poder de atualizar a lista de atividades consideradas de alto risco.

E é neste ponto que reside a maior diferença entre os dois dispositivos legais: enquanto o Regulamento Europeu concentrou o poder de reclassificação com o Poder Executivo, o Projeto de Lei Brasileiro organiza um sistema no qual, sem hierarquia entre os participantes, autoridade central e outros entes reguladores, inclusive com participação social.

10. Considerações Finais

A análise comparativa revela que tanto o Regulamento da UE quanto o PL 2338/2023 brasileiro compartilham uma espinha dorsal comum em sua abordagem à IA: uma estratificação baseada no risco. Ambos proíbem práticas consideradas inaceitáveis/excessivas e impõem um regime rigoroso para sistemas de alto risco, com um foco claro na proteção dos direitos fundamentais, saúde e segurança. A gestão de riscos é um processo contínuo e central para os desenvolvedores/fornecedores, e a avaliação de impacto sobre direitos fundamentais (FRIA na UE, AIA no Brasil) surge como um instrumento crucial de responsabilização para os utilizadores/aplicadores.

As divergências residem mais nas nuances da categorização (o PL brasileiro não formaliza explicitamente "riscos moderados/leves" com regimes distintos no seu capítulo de classificação, optando por uma gestão através de princípios gerais e mecanismos voluntários para o que está abaixo do alto risco). Também diverge quanto à competência para modificar a lista de atividades de IA consideradas de alto risco, e na maior densidade de especificidade das obrigações para certos atores da cadeia de valor (como mandatários e importadores, mais detalhados na UE).

Contudo, o objetivo convergente de criar um ambiente onde a IA possa ser desenvolvida e utilizada de forma confiável e benéfica para a sociedade, mitigando seus perigos, é evidente em ambas as propostas legislativas. Sob este ponto de vista, é louvável que o Senado Brasileiro tenha buscado inspiração na legislação europeia, que tanto buscou preservar os direitos fundamentais dos cidadãos, em detrimento da liberdade de desenvolvimento de IA de uma forma menos regulamentada.

Referências

BATISTA, Anderson Röhe Fontão; SANTAELLA, Lucia. Prognósticos das deepfakes na política eleitoral. **Organicom**, São Paulo, Brasil, v. 21, n. 44, p. 187–196, 2024. DOI: 10.11606/issn.2238-2593.organicom.2024.221294. Disponível em: https://revistas.usp.br/organicom/article/view/221294. Acesso em: 4 jun. 2025.

CAVALCANTI, Guilherme. PL da IA: Comissão mostra plano para definir política em 2025. **Agência Pública**, 28 de maio de 2025. Disponível em: https://apublica.org/nota/pl-da-ia-comissao-mostra-plano-para-definir-politica-em-2025/. Acesso em: 30 de maio de 2025.

COLOMBELLI, Wagner Godinho. **REGULAMENTAÇÃO DA IA (INTELIGÊNCIA ARTIFICIAL) NA ADMINISTRAÇÃO PÚBLICA BRASILEIRA**: Análise do Projeto de Lei N° 21 de 2020 e Projeto de Lei N° 2338 de 2023. 2024. 55 f. Trabalho de Conclusão de Curso (Graduação em Administração Pública e Políticas Públicas) - Instituto Latino-Americano de Economia, Sociedade e Política, Universidade Federal da Integração Latino-Americana, Foz do Iguaçu, 2024. Disponível em: https://revistatopicos.com.br/artigos/inteligencia-artificial-historia-tipologia-e-aplicacoes. Acesso em: 15 abril 2025.

CRAWFORD, Kate. ***The Atlas of AI***: Power, Politics, and the Planetary Costs of Artificial Intelligence. New Haven: Yale University Press, 2021.

EYSENCK, Michael W.; EYSENCK, Christine. ***AI vs Humans***. London: Routledge, 2022.

LOURENÇO, Luciano; AMARO, Antônio (Coords). **Riscos e Crises: da teoria à plena manifestação**. Coimbra: Imprensa da Universidade de Coimbra, 2018

MANTELERO, Alessandro. The Fundamental Rights Impact Assessment (FRIA) in the AI Act: Roots, legal obligations and key elements for a model template. **Computer Law & Security Review: The International Journal of Technology Law and Practice**, v. 54, 106020, 2024. Disponível em: https://doi.org/10.1016/j.clsr.2024.106020.

MORAES, Alexandre Rocha Almeida de; LISBOA, Andressa Felix. Regulamentação da Inteligência Artificial na União Europeia: estrutura ética, classificação de riscos e possíveis reflexos na medicina. **UNISANTA Law and Social Science**, v. 13, n. 2, p. 16-29, jul./dez. 2024. ISSN: 2317-1308.

PATRÃO, Afonso. O valor jurídico dos considerandos no direito da União Europeia: Reflexões a propósito da alegada imposição de acesso a mensagens de correio electrónico pela

Autoridade da Concorrência. *In*: LAVOURAS, Matilde; ALMEIDA, João Nogueira de; CALVETE, Victor; ALMEIDA, Teresa (Org.). **Boletim de Ciências Económicas**: Homenagem ao Prof. Doutor Manuel Carlos Lopes Porto. Coimbra: Faculdade de Direito, Universidade de Coimbra, 2023. v. LXVI, t. III, p. 2477-2502.

RUSSELL, Stuart. ***Human Compatible***: Artificial Intelligence and the Problem of Control. New York: Viking, 2019.

ZUBOFF, Shoshana. ***The Age of Surveillance Capitalism***: The Fight for a Human Future at the New Frontier of Power. New York: PublicAffairs, 2019.

Detalhes do(s) autor(a/es)

Henrique Silviano Almeida Viana

Mestrando em Direito pela Universidade Católica de Pernambuco, analista do Tribunal de Justiça de Pernambuco. E-mail:henrique.00000850015@unicap.br .

Stefano Gonçalves Régis Toscano

Doutor em Direito pela UFPE. Professor no PPGD na Universidade Católica de Pernambuco.