



ANÁLISE COMPARATIVA DO PROJETO DE LEI 2338/2023 COM ABORDAGENS REGULATÓRIAS INTERNACIONAIS: COMO EVITAR A LAVAGEM NA INOVAÇÃO E ABORDAR DE FORMA ADEQUADA NOVOS DIREITOS FUNDAMENTAIS COMO OS NEURODIREITOS E O DIREITO AO SONHO

COMPARATIVE ANALYSIS OF BILL 2338/2023 AND INTERNATIONAL REGULATORY APPROACHES: HOW TO PREVENT INNOVATION- WASHING AND PROPERLY ADDRESS NEW FUNDAMENTAL RIGHTS SUCH AS NEURO-RIGHTS AND THE RIGHT TO DREAM

PAOLA CANTARINI

RESUMO

O presente texto traz parte do parecer jurídico, elaborado por mim no âmbito do Instituto EthikAI e aberto a contribuições e debate da comunidade acadêmica vinculada ao CEADIN/USP e projeto UAI/IEA/USP, e visa, em suma trazer uma análise crítica, interdisciplinar, holística e comparativa do Projeto de Lei nº 2338/2023 em tramitação na Câmara dos Deputados com marcos normativos internacionais, além de trazer fundamentos na doutrina nacional e internacional. Parte-se de uma perspectiva técnico-normativa, ética e geopolítica, com ênfase na proteção de direitos fundamentais, na soberania tecnológica nacional e na compatibilização entre inovação e responsabilidade, fugindo de mantras como o de um necessário tradeoff entre tais temas, e evitando-se o que denominamos de "lavagem de inovação", a exemplo do que já ocorre com a ethics washing green e blue washing. O parecer propõe um equilíbrio regulatório substantivo, destaca lacunas do texto atual, e propõe ajustes inspirados em boas práticas internacionais, sem perder de vista as especificidades do Sul Global. Junta-se a teoria à prática concreta, e evita-se dar soluções simplistas para problemas complexos.

METODOLOGIA

A metodologia adotada é qualitativa, normativa e comparada, baseada na análise documental de:

- versões oficiais do PL 2338/2023 (Senado e Câmara),
- AI Act e AI Liability Directive (UE),
- documentos regulatórios do Reino Unido e Japão,
- literatura especializada (Floridi, Hoffmann-Riem, Zuboff, Pasquinelli),



Esta obra está licenciado com uma Licença [Creative Commons Atribuição-NãoComercial 4.0 Internacional](#).



- dados empíricos sobre impactos ambientais, econômicos e geopolíticos de infraestruturas de IA no Brasil e América Latina.

Complementa-se com abordagem interdisciplinar (jurídica, filosófica, técnica e política), incorporando contribuições de pesquisas realizadas no Observatório Brasileiro de Inteligência Artificial (OBIA) e diálogos realizados em Fortaleza por ocasião do encontro IBGE e PNUD “Novas fronteiras do desenvolvimento humano no século XXI – desafios e marcos para a governança da IA no Brasil, além de pesquisas que estamos realizando desde 2019 no âmbito do Instituto Ethikai (ethikai.org; revistaethikai.org), e de projetos que coordenamos no âmbito da temática da governança, com destaque para coordenação da equipe de governança durante a Cátedra Oscar Sala/IEA/USP e coordenação da equipe de governança para o projeto UAI/IEA/USP.

RESULTADOS

O parecer demonstra:

- A fragilidade de diversos dispositivos do PL 2338 na versão atual da Câmara, sobretudo no tocante à ausência de instrumentos concretos para assegurar proteção efetiva de direitos fundamentais em diversos pontos, fiscalização independente e mecanismos de compensação por danos.
- A falta de exigências mínimas a fornecedores estrangeiros instalados no Brasil (como data centers), resultando em risco de colonialismo computacional.
- A ausência de mecanismos obrigatórios como sandbox público, auditorias externas e avaliação de impacto algorítmico com participação social, e trazendo requisitos mínimos, proceduralização, obrigatoriedade de realização de forma prévia, em casos de risco alto, e incentivos claros e concretos para sua realização por startups e pequenas empresas.
- A insuficiência do modelo regulatório brasileiro para compatibilizar responsabilidade e inovação, embora no caminho certo neste sentido mas faltando medidas concretas e operacionais.

CONTRIBUIÇÕES

Entre as principais contribuições destacam-se:

- Proposta inovadora de reconhecimento do "direito aos sonhos" como novo direito fundamental vinculado aos neurodireitos e sugestão de um novo "bill of human rights" em face das exigências e atualizações que demandam a temática da IA.
- Formulação de um *framework* normativo de proteção a neurodireitos no contexto da IA.
- Denúncia da prática emergente de "lavagem da inovação" — paralela à ética-washing e greenwashing — em contextos regulatórios frágeis.
- Propostas de reciprocidade tecnológica, infraestruturas públicas de IA, sandboxes democráticos, e exigência de neutralidade climática para data centers.





- Sugestões para tornar o PL 2338 mais efetivo e justo, com base em experiências comparadas e princípios de justiça algorítmica, soberania digital e accountability público.

PALAVRAS-CHAVE: PL 2338/2023; Inteligência Artificial; AI Act; Neurodireitos; Soberania Tecnológica; Governança Algorítmica; Sandboxes Públicos; Lavagem da Inovação; Direitos Fundamentais; Sul Global.

ABSTRACT

This text presents part of the legal opinion I drafted within the scope of the EthikAI Institute, open to contributions and debate from the academic community affiliated with CEADIN/USP and the UAI/IEA/USP project. It aims to provide a critical, interdisciplinary, holistic, and comparative analysis of Bill No. 2338/2023, currently under review in the Brazilian Chamber of Deputies, juxtaposed with international regulatory frameworks, and grounded in both national and international legal doctrine.

The analysis is based on technical-normative, ethical, and geopolitical perspectives, emphasizing the protection of fundamental rights, national technological sovereignty, and the reconciliation between innovation and responsibility. It deliberately avoids oversimplified tradeoff narratives between these themes, and denounces what we term “innovation-washing,” analogous to ethics-washing, greenwashing, and bluewashing.

The opinion advocates for substantive regulatory balance, identifies key gaps in the current draft of the bill, and proposes adjustments inspired by international best practices while remaining attentive to the specificities of the Global South. It integrates theory with practical realities and resists offering simplistic solutions to complex problems.

METHODOLOGY

The methodology employed is qualitative, normative, and comparative, based on documentary analysis of:

- Official versions of Bill 2338/2023 (Senate and Chamber);
- The EU AI Act and AI Liability Directive;
- Regulatory frameworks from the United Kingdom and Japan;
- Specialized literature (Floridi, Hoffmann-Riem, Zuboff, Pasquinelli);
- Empirical data on the environmental, economic, and geopolitical impacts of AI infrastructures in Brazil and Latin America.

This is complemented by an interdisciplinary approach—legal, philosophical, technical, and political—incorporating insights from research conducted by the Brazilian Observatory of Artificial Intelligence (OBIA), discussions held in Fortaleza during the IBGE and UNDP event *“New Frontiers of Human Development in the 21st Century: Challenges and Frameworks for AI Governance in Brazil”*, and studies carried out since 2019 by the EthikAI Institute (ethikai.org; revistaethikai.org).

This work also draws from projects I have coordinated on AI governance, including the governance team under the Oscar Sala Chair/IEA/USP and the governance team for the UAI/IEA/USP project.





RESULTS

The opinion demonstrates:

- The fragility of several provisions of Bill 2338 in its current version in the Chamber, particularly regarding the lack of concrete mechanisms to ensure effective protection of fundamental rights, independent oversight, and damage compensation.
- The absence of minimum requirements imposed on foreign providers operating in Brazil (such as data centers), posing risks of computational colonialism.
- The lack of mandatory mechanisms such as public sandboxes, external audits, and algorithmic impact assessments with public participation, as well as the absence of minimum requirements, procedural rules, mandatory *ex ante* realization in high-risk cases, and concrete incentives for startups and small companies.
- The insufficiency of the current Brazilian regulatory model in harmonizing responsibility with innovation—despite being directionally sound, it lacks operational and concrete implementation measures.

CONTRIBUTIONS

Key contributions include:

- An innovative proposal for the recognition of the “right to dream” as a new fundamental right linked to neuro-rights, along with the suggestion of a new “bill of human rights” in response to the evolving demands posed by AI.
- The formulation of a normative framework for the protection of neuro-rights in the context of artificial intelligence.
- Denunciation of the emerging practice of “innovation-washing”—parallel to ethics-washing and greenwashing—particularly in weak regulatory environments.
- Proposals for technological reciprocity, public AI infrastructures, democratic sandboxes, and mandatory climate neutrality for data centers.
- Recommendations for making Bill 2338 more effective and equitable, based on comparative experiences and principles of algorithmic justice, digital sovereignty, and public accountability.

KEYWORDS: Bill 2338/2023; Artificial Intelligence; AI Act; Neuro-Rights; Technological Sovereignty; Algorithmic Governance; Public Sandboxes; Innovation-Washing; Fundamental Rights; Global South.

1 INTRODUÇÃO

O Projeto de Lei 2338/2023, aprovado pelo Senado Federal em dezembro de 2024 e atualmente em tramitação na Câmara dos Deputados, que estabelece o marco



Esta obra está licenciado com uma Licença [Creative Commons Atribuição-NãoComercial 4.0 Internacional](#).



regulatório para inteligência artificial no Brasil será analisado tendo em vista as seguintes dimensões centrais: lacunas e omissões, impacto ambiental, medidas pró-inovação com ênfase no sandbox regulatório, análise de risco e níveis de risco e avaliação de impacto algorítmico, comparando-as com o AI Act europeu, propostas do Reino Unido, Japão (UK AI Regulation White Paper (2023): <https://www.gov.uk/government/publications/a-pro-innovation-approach-to-ai-regulation> - Japan METI AI Governance Guidelines (2022): https://www.meti.go.jp/english/press/2022/0617_001.html) e novas iniciativas regulatórias da União Europeia publicadas em 2025 ((<https://digital-strategy.ec.europa.eu/en/funding/commission-launches-call-tender-part-efforts-establish-ai-act-service-desk>; <https://digital-strategy.ec.europa.eu/en/news/commission-sets-course-europes-ai-leadership-ambitious-ai-continent-action-plan>)). Frisa-se que o Instituto Ethikai já trouxe parte destas considerações em um primeiro draft enviado ao Senado Federal, mas agora a presente proposta traz maior robustez teórica.

Além disso como material complementar há uma proposta executiva publicada em nosso site (ethikai.org, revistaethikai.org) para se refletir acerca da estrutura de governança da IA em torno de um conceito amplo, além do que consta no PBIA, portanto, que reduziu o conceito à governança de dados e infraestrutura, à luz de importantes exemplos paradigmáticos e marcos teóricos (Virgilio Almeida e Urs Gasser, "A Layered Model for AI Governance", 2017, IEEE. Internet Computing, "The Oxford Handbook of AI Governance", Oxford University Press, 2024), trazendo importantes medidas em torno de políticas públicas, meio ambiente, educação e infraestrutura, a fim de complementar a proposta legislativa.

O Projeto de Lei nº 2338/2023 apresenta, em suma, oportunidades e riscos, avanços e retrocessos. A comparação com o *AI Act* da União Europeia, com o *AI Liability Directive*, e com os modelos regulatórios do Reino Unido e do Japão, revela boas práticas, lacunas regulatórias e direções estratégicas, mas deverá ser reformado em diversos pontos para poder se falar em um modelo de regulação brasileiro robusto e que traga ao mesmo tempo proteção adequada a direitos fundamentais e incentivos à inovação. Este documento traz uma análise técnica exaustiva e recomendações com base em evidências normativas, empíricas e políticas, incluindo os impactos ambientais, econômicos e geopolíticos da IA no Brasil como país do Sul Global.





Sugestões preliminares - Análise Comparativa com Abordagens Regulatórias Internacionais e Problemas identificados

O Brasil deve negociar ativamente sua posição no mapa global da IA, não apenas como consumidor e infraestrutura barata, mas como agente soberano que define contrapartidas, regula com base em direitos e exige transferência de valor real para a sociedade. A instalação de data centers vista como medida pró inovação deve ser condicionada à proteção dos dados, da soberania e da justiça ambiental e social. A inovação deverá ser tratada de forma séria, portanto, evitando-se também neste âmbito o que já ocorre no âmbito da ética, do meio ambiente e do compliance, com os nomes respectivos de ethics washing, green washing e blue washing.

Evitariamos com isso o que se poderia denominar de **innovation washing** na linha do que dispõem Luciano Floridi e Michael Veale ao falar do *ethics washing* e evitariamos o *Data Colonialism* (Nick Couldry e Ulises Mejias). O innovation washing se daria com o uso instrumental e retórico da “inovação” como justificativa para práticas tecnológicas que, na prática, violam direitos, concentram poder e aprofundam desigualdades — ao mesmo tempo em que encobrem tais efeitos sob discursos de progresso, inclusão ou neutralidade. É o que apontam autores como: **Shoshana Zuboff** – *The Age of Surveillance Capitalism (The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.* PublicAffairs, 2019), **Kate Crawford** (*Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence*. Yale University Pres, 2021), **Ruha Benjamin** (*Race After Technology: Abolitionist Tools for the New Jim Code*. Polity Press, 2019), **Evgeny Morozov** (*To Save Everything, Click Here: The Folly of Technological Solutionism*. PublicAffairs, 2013), **Virginia Eubanks** (*Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. St. Martin’s Press, 2018), **Jathan Sadowski** (*Too Smart: How Digital Capitalism is Extracting Data, Controlling Our Lives, and Taking Over the World*. MIT Press, 2020).

O Brasil deve, pois, evitar a **dependência total** – que traz riscos de **colonialismo computacional** e submissão aos interesses geopolíticos estrangeiros e para isso é essencial o desenvolvimento de infraestrutura própria (mesmo que menor) como **condição de soberania**, como saúde ou defesa nacional. O Brasil possui capacidade para liderar alternativas para o Sul Global, trazendo um modelo alternativo de IA: ético,



voltado ao bem comum, à inclusão social, à democracia e ao meio ambiente. Com isso será um ponto central de **referência em dados culturais, linguísticos, ambientais e sociais do Sul**, criando modelos finetuned para suas realidades. Diante de suas já existentes vantagens competitivas e cooperação regional, **o Brasil tem potencial de liderança regional com América Latina e África em coalizões Sul-Sul e poderá liderar infraestruturas federadas, multilíngues e distribuídas (em edge AI, por exemplo)**.

Destacam-se iniciativas neste sentido como da França a exigir compensações ambientais e transparência energética dos data centers, da Índia a exigir armazenamento local de dados críticos, do Quênia, ao requerer investimentos sociais e em infraestrutura digital e da EU, consoante regras do AI Act, Data Act e Digital Services Act. Deve ser pensada a obrigatoriedade de medidas como *data trusts públicos*, infraestruturas cívicas de IA e accountability algorítmico público. Caso contrário será um modelo extrativista e colonial.

Com base em tais argumentos, seguem algumas sugestões preliminares:

- Tornar auditoria externa – AIA- avaliação de impacto algorítmico independente (auditoria de terceira parte), prévia e obrigatória para sistemas de alto risco (como o AI Act da UE). A auditoria deve ir além de análises técnicas, deve haver previsão de **auditorias públicas e participativas** para verificar o impacto real da IA nas condições de trabalho, direitos civis e democracia. Avaliações de Impacto Algorítmico obrigatórias com participação pública: prever a inclusão de mecanismos de consulta pública, revisão por pares e auditoria social participativa nas etapas da AIA.
- Podem ser incorporadas diretrizes como “*Fundamental Rights Impact Assessment*” (FRIA) e *Ethical AI Checklists*.
- Criar sandboxes públicos com financiamento transparente e independente trazendo de forma expressa isenção de sanções durante o mesmo e melhor especificações dos pontos aqui trazidos abaixo.
- Condicionar benefícios fiscais, treinamento e capacitação específica, treinamento em linguagem nacional, a reciprocidade tecnológica e soberania de dados, quando



se tratar de data centers instalados no país, sob pena de ter-se uma abordagem colonial.

- Trazer incentivos concretos mencionados para redirecionamento da IA que irá complementar e não substituir o trabalho humano: **trazer propostas** de incentivos tributários e públicos obrigatórios para **modelos de IA que ampliem as capacidades humanas**, melhorando a produtividade com inclusão.
- Trazer previsão de **tributação progressiva sobre os ganhos de produtividade oriundos da IA**, com redistribuição para políticas públicas de educação, saúde e infraestrutura digital.
- Trazer previsão de medidas concretas em prol da **educação e capacitação para o século XXI, a exemplo de medidas em que exijam que** os lucros gerados por IA sejam usados para financiar **capacitação digital, acesso a internet de qualidade e ensino técnico-científico inclusivo**.
- Desenvolvimento de **infraestruturas públicas ou cooperativas de IA**, com controle democrático, como alternativa à dependência das big techs. Infraestrutura de dados pública e interoperável (com soberania local).
Criação de uma nuvem soberana nacional (como o projeto **GAIA-X** na União Europeia) para garantir que os dados de cidadãos e do setor público não sejam transferidos para jurisdições sem proteção adequada.
Desenvolvimento de padrões abertos e interoperáveis para bancos de dados públicos (saúde, educação, mobilidade, justiça), com controle distribuído e transparência.
- **medidas de compensação e exigência, na forma de contrapartidas para os datacenteres instalados no país**

- contrapartidas obrigatórias

- Investimento obrigatório em **educação técnica local**, centros de P&D públicos e capacitação de mão de obra brasileira.
- Financiamento de hubs de inovação em universidades e fomento a **startups nacionais de IA ética**.

- tributação justa e redistributiva





- Evitar isenções fiscais amplas: exigir contribuição ao **Fundo Nacional de Inclusão Digital e Justiça Algorítmica a ser criado**.
- Estabelecer royalties ou impostos progressivos sobre lucros operacionais de data centers e exportação de dados.

- acesso e governança dos dados

- Exigir **data trusts soberanos**: dados gerados no Brasil devem ser armazenados localmente e tratados com supervisão brasileira.
- Estabelecer **cláusulas de soberania de dados** e impedir exportação não autorizada de bases sensíveis.

- compensação ambiental

- Cálculo e **compensação obrigatória da pegada hídrica e energética** dos data centers.
- Financiamento de projetos de **transição energética local** e reflorestamento com monitoramento público.

- exigência de neutralidade climática para data centers

- Aprovação de normas ambientais específicas para eficiência energética de servidores (uso de água, emissão de carbono, refrigeração).
- Compensação de pegada de carbono com obrigação de contribuição para projetos de energia limpa locais.
- Publicação obrigatória de relatórios ambientais por parte das empresas.

- trazer cláusulas de reciprocidade para Big Techs: dados por investimento público

- Implementar exigência legal para que empresas que queiram explorar dados brasileiros ou instalar data centers façam contrapartidas públicas:
 - investimento em infraestrutura científica nacional
 - repasse de parte dos lucros em royalties de dados
 - parceria obrigatória com universidades públicas.
- Data centers e empresas devem submeter-se a **Avaliação de Impacto Algorítmico (AIA)** e auditorias externas com foco em direitos humanos e impacto em grupos vulneráveis, observando os critérios já expostos aqui.



- Redes descentralizadas de Edge AI com foco territorializado por meio do fomento a infraestruturas de computação de borda (edge computing) operadas por universidades, comunidades, cooperativas, prefeituras.
- Descentralização da inteligência artificial para que análises de dados ocorram localmente, com autonomia e foco em soluções comunitárias (ex: saúde pública, agricultura familiar, mobilidade urbana).
- Consolidar a ANPD como núcleo regulador e criar instância multisectorial e com atenção à diversidade epistêmica, de supervisão, e repensar o modelo de fragmentação em diversas autoridades setoriais, sem expertise em IA.
- O PL 2338/2023 acerta em trazer diretrizes para inovação, mas carece de instrumentos legais e administrativos para sua efetivação. A inovação precisa ser protegida e fomentada com medidas positivas claras e exequíveis, não apenas com declarações de princípios.
- A ausência de uma autoridade central com competência clara compromete a efetividade da regulação e a segurança jurídica. Ausência de autoridade central clara com poder de voto normativo. Risco de fragmentação regulatória: diferentes agências podem divergir em seus entendimentos, sem coordenação. Neste sentido no AI Act, as práticas proibidas são taxativamente definidas pelo Parlamento Europeu, e a Comissão Europeia coordena com os Estados-membros sua implementação. Tal gap poderia ser contornado com a criação de uma autoridade nacional coordenadora de IA com competência para:
 - Emitir pareceres vinculantes sobre proibição de sistemas;
 - Harmonizar a atuação dos reguladores setoriais;
 - Articular com ANPD, CGI.br, CNPD, etc.
- Falta de definição normativa de “risco excessivo”: o conceito não é operacionalizável tal como redigido. Tal gap poderia ser resolvido com a definição legal do que constitui “risco inaceitável”, à semelhança do Art. 5 do AI Act, com: Critérios técnicos e direitos fundamentais protegidos.

Pontos de destaque

1. Análise e classificação de risco





O PL se apoia no conceito de inovação responsável (Wolfgang Hoffmann-Riem) e de forma a conjugar inovação e ética (Luciano Floridi – metainnovation). O projeto adota uma abordagem baseada em risco e em direitos, mas de forma proporcional e mais flexível que o AI Act, segundo parte da doutrina majoritária (salvo alguns entendimentos opostos a exemplo do ITSARIO (<https://itsrio.org/pt/publicacoes/relatorio-analise-da-relacao-entre-o-pbia-e-o-pl-para-regular-a-ia-estretegias-em-conflito/>;<https://itsrio.org/pt/publicacoes/100-ia-pl-2338-e-a-classificacao-de-riscos-dos-usos-de-ia-sob-uma-perspectiva-pratica/>), ou seja, busca assim como o AI Act ressalta, balancear inovação e proteção adequada a direitos fundamentais. Contudo, no artigo 5º são elencados de forma expressa somente alguns direitos fundamentais, como se observa dos incisos II (direito à privacidade e à proteção de dados pessoais) e III (direito à não discriminação).

Resta analisar, em suma, os seguintes pontos:

- **O PL 2338 é mais abrangente e mais exigente do que o AI Act?**
- **Impõe obrigações mais genéricas e menos calibradas por risco?**

Enquanto o AI Act em seu art. 5 proíbe expressamente sistemas de IA incompatíveis com os direitos fundamentais (como manipulação subliminar, exploração de vulnerabilidades, e scoring social) e traz categorias de sistemas de alto risco com base no impacto sobre saúde, segurança e direitos fundamentais, o *PL 2338* não estrutura a classificação de risco com base no impacto sobre direitos fundamentais — mas sim em setores e finalidades, o que poderia fragilizar o arcabouço protetivo.

O modelo brasileiro não apresentaria taxonomia clara e estruturada de risco, nem estabeleceria obrigações diretamente proporcionais ao nível de risco dos sistemas?

Enquanto o AI Act traz quatro níveis de risco (proibido, alto risco, risco limitado e risco mínimo), impondo para os sistemas de “alto risco” obrigações rigorosas (Art. 16–29), o PL 2338 traz apenas 3 níveis, e adota um conceito genérico de “sistemas de IA de alto risco” (Art. 7º); não há gradação clara como no AI Act. A definição é excessivamente aberta, e a lista de sistemas de alto risco carece de clareza conceitual, podendo comprometer a aplicabilidade prática e a segurança jurídica.





Contudo, acerca da afirmação de que o PI 2338 teria previsto mais obrigações para os riscos mais baixos do que o AI ACT, como alguns apontam, não parece se sustentar; contudo mereceria uma revisão as categorias de risco em alguns pontos centrais a fim de verificar a calibragem de forma a serem proporcionais as obrigações ao nível de risco e trazer maior conceituação e lista clara de quais riscos são em quais níveis. O PL é menos objetivo acerca de quais aplicações de IA se enquadram em cada nível de risco, ensejando diversas interpretações e mais insegurança jurídica. Portanto, o PL é mais vago e menos calibrado por risco, devendo ser revista tal parte, a fim de trazer a proporcionalidade entre nível de risco e obrigações. Também deverá analisar a necessária previsão de incentivos para o compliance de startups e pequenas empresas que deverão elaborar como medida mitigadora de risco alto a AIA de forma obrigatória. Seria interessante trazer uma nova classificação intermediária, com riscos médio e baixo como no AI ACT.

Enquanto que o AI Act traz uma lista taxativa e exaustiva de sistemas expressamente proibidos, o PI dispõe em seu artigo 13 os riscos excessivos vedando o desenvolvimento, a implementação e o uso de sistemas de IA, I – com alguns propósitos delineados.

Por sua vez dispõe o § 2º que “o uso de sistemas a que se refere o inciso IV deste artigo deverá ser proporcional e estritamente necessário ao atendimento do interesse público, observados o devido processo legal e o controle judicial, bem como os princípios e direitos previstos nesta Lei e, no que couber, na Lei no 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), especialmente a garantia contra a discriminação e a necessidade de revisão da inferência algorítmica pelo agente público responsável” (sugestão: garantia de respeito a todos os direitos fundamentais potencialmente afetados, e exigência de elaboração prévia de AIA de forma independente).

Seria interessante ainda trazer, a exemplo do AI Act, as seguintes proibições expressas: sistemas de categorização biométrica baseados em características sensíveis (como origem étnica, opiniões políticas, religião, etc.) – AI Act, Art. 5(1)(a); sistemas de pontuação social generalizada (social scoring) por autoridades públicas – AI Act, Art. 5(1)(b).



Já o PL considera alto risco no seu artigo 14 dispondo: “considera-se de alto risco o sistema de IA empregado para as seguintes finalidades e contextos de usos, levando-se em conta a probabilidade e a gravidade dos impactos adversos sobre pessoas ou grupos afetados, nos termos de regulamentação”.

Observação e sugestão: além da probabilidade e gravidade, devem ser levados em conta outros fatores:

Irreversibilidade dos danos

Por que é importante: Algumas consequências da IA são definitivas ou de difícil remediação, como violações de neurodireitos, discriminação automatizada com efeitos cumulativos, ou danos ambientais irreparáveis.

Exemplo prático: Um sistema que gera decisões judiciais enviesadas ou que influencie resultados eleitorais não pode ser simplesmente “corrigido” depois — o dano histórico permanece.

2. Escala do impacto

Quantas pessoas ou sistemas são afetados?

Um sistema de IA usado por milhões de cidadãos (ex: benefícios sociais, segurança pública, educação pública) terá impacto muito mais difuso e sistêmico que um sistema usado por uma única empresa.

3. Persistência temporal do risco

O dano é contínuo? Ou é pontual e controlável?

Exemplo: Sistemas de vigilância em larga escala ou de perfilamento preditivo tendem a gerar riscos persistentes ao longo do tempo.

4. Grau de opacidade ou explicabilidade

Quanto mais inexplicável ou opaco for o sistema, maior o risco à accountability e à contestação de decisões — sobretudo em áreas sensíveis como justiça, saúde, crédito, segurança pública.

5. Assimetria de poder e vulnerabilidade dos afetados

É essencial considerar quem está mais exposto aos danos da IA:

Crianças, pessoas racializadas, populações periféricas, migrantes, etc.

Exemplo: Um sistema de triagem de currículos pode amplificar desigualdades já existentes se usado sem critérios justos.





6. Capacidade de contestação / remediação

Há meios concretos de revisar ou corrigir uma decisão automatizada?

A ausência de mecanismos de revisão humana ou contestação aumenta o risco ético e jurídico.

7. Potencial de uso dual ou indevido

Um sistema pode ser usado para fins diferentes dos inicialmente propostos, inclusive abusivos?

Ex: Reconhecimento facial criado para autenticação bancária ser usado para vigilância estatal.

8. Dependência sistêmica

O sistema afeta infraestruturas críticas (saúde, energia, segurança pública, finanças)?

Riscos nesses setores podem ter efeito em cadeia ou ser catalisadores de outras vulnerabilidades.

Sugestão de fórmula para avaliação de risco de IA (ampliada):

Risco = Probabilidade x Gravidade x Escala x Irreversibilidade x (1 - Transparência)

(Ajustada por fatores de vulnerabilidade, dual use, contestabilidade e setor crítico)

Propostas de Aprimoramento para o PL 2338/2023

Para fortalecer o PL 2338/2023, considerando as melhores práticas internacionais:

1. Definir explicitamente práticas proibidas: Incluir uma lista clara de práticas de IA proibidas, alinhada ao Artigo 5 do AI Act, para evitar ambiguidades e garantir a proteção dos direitos fundamentais.
2. Adotar uma classificação de risco mais granular: Considerar a introdução de categorias adicionais, a exemplo: "risco limitado" e "risco mínimo", seguindo o modelo quadripartite do AI Act, para evitar que obrigações desproporcionais sejam aplicadas a sistemas de baixo impacto.
3. Estabelecer critérios objetivos para cada categoria de risco: O PL deveria incorporar critérios técnicos e setoriais mais precisos (como os Anexos II e III do AI Act), evitando subjetividades na classificação do risco como



“alto”. Trazer critérios e balizamentos protetivos para a reclassificação pela autoridade competente, sob pena de esvaziar a proteção apresentada.

4. Melhor definir as obrigações regulatórias por categoria de risco: O atual texto brasileiro impõe um número elevado e pouco hierarquizado de obrigações para sistemas de alto risco. Seria mais eficiente e justo se o texto:

- Diferenciasse obrigações entre tipos de agentes (startups, pequenas empresas, grandes plataformas);
- Alinhasse os requisitos a modelos de “accountability proporcional”, como os previstos na LGPD e nos padrões internacionais;
- Trazer incentivos claros para as startups, pequenas empresas elaborarem AIA.

2. Excesso de delegação posterior e falta de expertise em IA dos reguladores setoriais

O PI apresenta riscos de captura regulatória ao transferir poderes para reguladores setoriais sem clara definição de competências, inclusive sem exigir capacitação em IA destas as quais não possuem expertise em tal temática. No tocante à falta de expertise em IA dos reguladores setoriais, por exemplo, essa é uma das principais críticas feitas à abordagem do Reino Unido (“AI Regulation: A Pro-Innovation Approach”, 2023). A resposta britânica envolve: mecanismos compensatórios no modelo do Reino Unido/ capacitação técnica intersetorial. O governo criou o UK AI Standards Hub e está financiando formação técnica de reguladores. Função do novo “Central AI Function” - Um núcleo técnico nacional que suporta os reguladores setoriais com frameworks e ferramentas. Guias técnicos e regulatórios comuns - Reguladores usam guidelines centralizadas para mitigar lacunas de especialização. O modelo britânico reconhece a limitação técnica e tenta mitigá-la com centralização do conhecimento, sem tirar dos reguladores a competência decisória — o que ainda é polêmico e em avaliação.

3. Novos direitos previstos

O PL avança com a previsão do **devido processo informacional, mas deixa de prever outros importantes direitos como privacidade em grupo** (diante da





preocupação do caso dos “data brokers”), inferências razoáveis, e neurodireitos. Neste contexto trazemos nossa contribuição epistemológica e metodológica conforme artigos já publicados no Jornal USP, Coluna Migalhas e Coluna TropicAI da Academia Baiana de Letras, e constante dos livros “Filosofia da IA” e “Governança da IA com base nos valores construcionistas do homo poieticus” (Lumen Juris, 2024), objeto de pesquisas em sede de diversos pós-doutorados realizados na USP, na PUC, na Universidade Reggio Calabria, na Universidade de Coimbra em IA, direitos humanos e fundamentais e epistemologias do sul, e experiências práticas no âmbito da Cátedra Oscar Sala coordenando a equipe de governança, no Projeto UAI do IEA – Instituto de Estudos Avançados/USP, coordenando a equipe de governança, e com pesquisas realizadas no âmbito do OBIA – Observatório Brasileiro de IA.

A Nova Fronteira dos Direitos Fundamentais e Humanos, Neurocapitalismo e a Mercantilização dos Dados Neurais

Novo “Bill of human rights”, neurodireitos e direito ao sonho

Com fundamento em autores como Sandra Wachter, Brent Mittelstadt (“A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI.” Columbia Business Law Review, 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3248829), Helen Nissenbaum (“Privacy in Context: Technology, Policy, and the Integrity of Social Life.” Stanford University Press, 2010), Luciano Floridi (“Group Privacy: A Defence and an Extension.” Philosophy & Technology, 2014. <https://link.springer.com/article/10.1007/s13347-014-0157-2>), Daniel Solove e sua teoria sobre o devido processo informacional vinculado à proteção de privacidade (Daniel J. Solove, “The Digital Person: Technology and Privacy in the Information Age.”, 2004), e ainda com base em Habermas e em Martha Nussbaum, afirmamos a necessidade do reconhecimento de novos direitos fundamentais.

O século XXI apresenta desafios inéditos à dignidade humana que transcendem as categorias tradicionais dos direitos humanos estabelecidas no pós-guerra. A revolução



digital, os avanços em neurociência, a inteligência artificial e as novas formas de organização social criaram lacunas normativas que exigem uma reformulação profunda do marco jurídico-filosófico dos direitos fundamentais e humanos. É urgente o reconhecimento de novos direitos humanos e fundamentais emergentes e a construção de um novo “Bill of Human Rights” adaptado às realidades contemporâneas, fundamentado nos trabalhos de pensadores contemporâneos que têm dedicado suas carreiras a compreender e responder a esses desafios.

As rápidas inovações em neurociência e interfaces cérebro-máquina (Brain-Computer Interfaces – BCIs) inauguram uma nova fronteira no campo dos direitos humanos. Tecnologias capazes de ler, decodificar, manipular e estimular a atividade cerebral colocam em risco a autodeterminação mental, a privacidade cognitiva e a integridade psíquica dos indivíduos. A literatura contemporânea já identifica a necessidade de uma nova geração de direitos fundamentais e humanos – os neurodireitos – como resposta normativa a tais desafios (Yuste et al., 2017; Ienca & Andorno, 2017).

O neurocapitalismo representa uma nova configuração de poder, na qual dados cerebrais são extraídos, armazenados, processados e comercializados com finalidade de lucro, ampliando as já existentes assimetrias profundas entre indivíduos e corporações.

O avanço das neurotecnoLOGIAS demanda uma profunda atualização do catálogo de direitos fundamentais e humanos. A privacidade cerebral, o direito ao sonho e a limitação do neurocapitalismo são apenas as primeiras expressões dessa transformação normativa necessária.

O reconhecimento dos neurodireitos representa não apenas uma resposta a riscos emergentes, mas também um compromisso ético com a preservação da autonomia, da dignidade e da liberdade cognitiva dos indivíduos em um mundo cada vez mais invasivo e neuroinformacional.

O direito à privacidade cerebral refere-se à proteção jurídica da atividade elétrica, química e funcional do cérebro, incluindo os dados derivados de sua captação, análise e inferência por tecnologias neurocientíficas. Trata-se de um desdobramento direto da proteção de dados pessoais, porém com um grau de sensibilidade e risco inédito.



A atividade neural contém informações sobre emoções, crenças, memórias e até intenções futuras. Tal conteúdo, caso seja acessado sem consentimento ou processado de forma inadequada, pode violar os direitos à intimidade, à autodeterminação informacional e à liberdade de pensamento, configurando uma nova forma de vigilância cognitiva (lenca & Andorno, 2017).

Neurodireitos são um conjunto emergente de direitos fundamentais que visam proteger a integridade, a autonomia e a liberdade mental dos indivíduos diante do avanço das neurotecnologias e da interface direta entre cérebro e máquina (Brain-Computer Interfaces – BCIs), além de tecnologias de leitura, manipulação ou alteração da atividade cerebral.

São neurodireitos fundamentais (Yuste, R., Goering, S., et al., "Four ethical priorities for neurotechnologies and AI.", 2017, *Nature*, 551(7679), 159–163):

Direito à Privacidade Mental: A proteção das informações pessoais obtidas através de neurotecnologias (neurodados) contra decodificação sem consentimento prévio;

Direito à Identidade Mental: O direito à consciência e à manutenção da identidade pessoal contra alterações não autorizadas através de intervenções neurotecnológicas;

Direito à Liberdade Cognitiva (Cognitive Liberty)/Direito à Agência: A proteção da autonomia da vontade e da capacidade de tomada de decisões livres;

Direito à Integridade Mental/ Direito ao Livre Arbítrio: A preservação da capacidade de escolha independente contra manipulações neurais;

Direito ao Aprimoramento Cognitivo: A liberdade de escolher usar ou recusar tecnologias de aprimoramento mental;

Direito à Não-Discriminação Algorítmica com Base em Dados Neurais (Fair Access to Mental Augmentation).

Entre as iniciativas legislativas e constitucionais no mundo há o pioneirismo do Chile, como primeiro país a iniciar a constitucionalização dos neurodireitos incluindo em sua reforma constitucional de 2021 apontando para o direito à integridade física e mental e à proteção de dados neurais como direitos fundamentais explícitos na Constituição (<https://www.bcn.cl/leychile>). Na União Europeia o tema já aparece nos debates do Conselho Europeu de Bioética, no AI Act e no AI Liability Directive, com preocupação sobre IA e manipulação de processos cognitivos.



Nos Estados Unidos há projetos de lei em debate, especialmente em nível estadual (ex.: Califórnia), e discussões no âmbito da Neuroethics Initiative da National Institutes of Health (NIH).

A UNESCO na Recomendação sobre Ética da Inteligência Artificial – 2021 inclui o tema da proteção à privacidade mental como parte da agenda ética para IA.

O século XXI é marcado pela emergência de tecnologias capazes de acessar, decodificar e manipular a atividade cerebral humana. Interfaces cérebro-máquina, dispositivos de neuroestimulação e técnicas de neuromarketing avançado configuram um cenário onde as fronteiras entre pensamento, decisão e intervenção externa tornam-se cada vez mais tênues. Tal contexto demanda uma urgente ampliação do catálogo de direitos fundamentais e humanos, incorporando neurodireitos que protejam a autonomia, a dignidade cognitiva e a liberdade mental.

Empresas de tecnologia já desenvolvem produtos capazes de captar sinais neurais para fins de publicidade direcionada, modulação de comportamento do consumidor e análise de estados emocionais. As práticas de neurodata mining, nas quais dados cerebrais são coletados, armazenados e vendidos, criam uma nova categoria de risco social: a vigilância neurocognitiva. Essa forma de exploração extrapola os limites da privacidade tradicional, atingindo dimensões profundas da subjetividade humana.

Do ponto de vista jurídico, tal cenário representa uma violação não apenas da autodeterminação informacional (Floridi, 2014), mas também dos princípios constitucionais da dignidade da pessoa humana e da liberdade de pensamento.

A categoria emergente do direito denominado “Brain Data Privacy” busca estabelecer salvaguardas normativas para proteger informações derivadas da atividade cerebral, independentemente de sua identificação direta com o indivíduo. Trata-se de um direito que transcende a lógica tradicional da proteção de dados pessoais, reconhecendo o caráter sensível, íntimo e estruturalmente ligado à identidade dos dados neurais.

Plataformas de neurogames, dispositivos wearable para meditação ou produtividade e até aplicativos de análise de humor baseados em EEG (eletroencefalografia) já coletam tais dados. A ausência de regulação adequada cria um ambiente propício à exploração econômica da mente humana, com potenciais violações de privacidade, liberdade de pensamento e dignidade cognitiva.





São modalidades de exploração neurocapitalista:

- 1) o neuromarketing direto - empresas como a Neurosky já comercializam dispositivos de EEG consumer-grade para análise de resposta neural a estímulos publicitários. Esta "leitura direta" das preferências neurais representa salto qualitativo em relação ao marketing tradicional, prometendo acesso aos "verdadeiros" desejos do consumidor, não filtrados pela consciência reflexiva (<https://neurosky.com>);).
- 2) Otimização Cognitiva Comercial - plataformas como Nootopia, Brain.fm e Focus@Will vendem promessas de enhancement cognitivo através de estimulação neural, criando mercados de capacidades mentais onde atenção, memória e criatividade tornam-se commodities (<https://nootopia.com>; <https://www.brain.fm>; <https://www.focusatwill.com>).
- 3) Economia da Atenção Neural - dispositivos de monitoramento contínuo da atenção, como aqueles desenvolvidos pela BrainCo, permitem quantificação e mercantilização em tempo real dos recursos atencionais, criando novos mercados de "tempo mental".

O neurocapitalismo opera através de três mecanismos centrais de acumulação e expropriação:

- 1) Extração Neural: Captura de dados cerebrais através de dispositivos invasivos e não-invasivos, frequentemente sob pretexto terapêutico ou de enhancement.
- 2) Processamento Algorítmico: Aplicação de machine learning e IA para decodificação de padrões neurais e criação de perfis mentais detalhados.
- 3) Instrumentalização Comportamental: Uso de insights neurais para influência e modificação de comportamentos, criando loops de feedback que amplificam o controle sobre processos mentais.

Os dados cerebrais possuem características únicas que os distinguem categoricamente de outras formas de dados pessoais, tais como:

1) Involuntariedade Radical - diferentemente de dados comportamentais digitais, que resultam de ações conscientes (clicks, posts, compras), os dados neurais são produzidos involuntariamente pelos processos cerebrais básicos. O indivíduo não pode simplesmente "parar" de produzir ondas cerebrais ou atividade neural.

2) Acesso a Estados Mentais Privados - neurotecnologias contemporâneas permitem acesso a estados mentais que o próprio indivíduo pode não reconhecer





conscientemente, incluindo processos pré-conscientes, emoções implícitas e intenções não articuladas.

3) Imutabilidade Biométrica - Padrões neurais individuais apresentam características biométricas únicas e relativamente estáveis, funcionando como "impressões digitais cerebrais" que não podem ser alteradas voluntariamente.

O avanço das neurotecnoLOGIAS tem gerado um cenário de profundas transformações nas relações entre ciência, mercado e direitos fundamentais. Tais desafios e particularidades demonstram a inadequação dos Frameworks existentes a começar pelas limitações do modelo de consentimento, já que quase nunca se tem um consentimento livre, informado, granular e, pois, qualificado (fíCÇÃO do consentimento). O paradigma do consentimento central ao GDPR, LGPD e legislações similares, revela-se inadequado tanto para o contexto original e muito mais para dados neurais devido a várias razões:

- Impossibilidade de granularidade: Não é possível consentir seletivamente com tipos específicos de atividade neural
- Desconhecimento do escopo: Indivíduos não compreendem plenamente que informações podem ser extraídas de seus padrões neurais
- Permanência da extração: Uma vez estabelecida interface neural, a extração de dados torna-se contínua e dificulta revogação de consentimento
- Insuficiência da anonimização já que técnicas tradicionais de anonimização se mostram ineficazes para dados neurais devido à:
 1. Singularidade dos padrões cerebrais: Impossibilidade prática de verdadeira anonimização
 2. Capacidade de re-identificação: Algoritmos podem re-identificar indivíduos através de padrões neurais únicos
 3. Inferência de atributos sensíveis: Dados neurais "anonimizados" podem revelar orientação sexual, condições médicas, crenças políticas

Tendo em vista tais desafios, insuficiência do "status quo" do Direito para proteção adequada destes novos direitos propomos um framework específico e uma nova



dimensão dos novos neurodireitos, ao lado do direito à privacidade cerebral (Brain Data Privacy), o direito ao sonho como expressão da liberdade psíquica.

Deverá, pois, ser delineada uma Nova Gramática dos Direitos Humanos - Novo neurodireito fundamental: direito ao sonho - Liberdade Onírica como Direito Fundamental.

O direito ao sonho emerge como uma resposta aos primeiros experimentos de manipulação de conteúdos oníricos por meio de estimulação cerebral direcionada durante o sono (Tassi et al., 2021). Trata-se da proteção da autonomia psíquica durante os estados inconscientes, reconhecendo o sonho como espaço inviolável de liberdade mental e integridade subjetiva.

Inspirado nos princípios da liberdade de pensamento (Art. 18 da Declaração Universal dos Direitos Humanos) e da inviolabilidade da mente, este direito busca evitar intervenções tecnológicas que possam alterar, manipular ou comercializar experiências oníricas sem consentimento.

Pesquisas em Targeted Memory Reactivation (TMR) e similares já demonstram a capacidade de alterar conteúdos dos sonhos de forma dirigida. Grandes empresas de tecnologia têm financiado projetos voltados para "ad-driven dream manipulation", levantando sérias preocupações éticas.

A construção de um novo constitucionalismo cognitivo, capaz de proteger as liberdades mentais e psíquicas, torna-se imperativa frente ao avanço de práticas de extração, manipulação e monetização de dados cerebrais. O futuro dos direitos humanos fundamentais passa, inevitavelmente, pela proteção da mente.

Como contribuição essencial postulamos por outro neurodireito fundamental: o direito ao sonho como uma dimensão particularmente inovadora dos neurodireitos. À medida que as tecnologias de monitoramento neural se tornam capazes de acessar e interpretar a atividade cerebral durante o sono, torna-se essencial proteger este último refúgio da privacidade mental absoluta.

A mente humana como a última fronteira. Este direito engloba múltiplas dimensões:

- o direito de sonhar sem interferência externa;
- a proteção contra a leitura ou gravação de sonhos;
- o direito ao esquecimento onírico;





- a vedação da manipulação artificial dos conteúdos dos sonhos.

O sonho representa o último território verdadeiramente privado da experiência humana, e sua proteção jurídica simboliza a resistência à colonização total da mente humana pela tecnologia.

Jürgen Habermas, em seus trabalhos sobre direitos humanos e dignidade humana fornece fundamentos filosóficos para compreender como os direitos humanos devem evoluir em resposta a novos desafios. Habermas argumenta que a dignidade humana é o fundamento moral dos direitos humanos, mas que sua interpretação e aplicação devem ser constantemente reelaboradas em resposta a novas ameaças. Para Habermas os direitos humanos são um "projeto em aberto" que deve responder às transformações históricas e a dignidade humana está fundamentalmente ligada à nossa capacidade de **comunicação e reconhecimento mútuo**. Da mesma forma no âmbito dos direitos fundamentais, a exemplo do reconhecimento recente da proteção de dados como um direito expresso no rol do artigo 5º da CF. Na esfera informacional isso se traduz em estarem presentes as seguintes condições de comunicação livre: ausência de coerção, simetria comunicativa, e transparência; o reconhecimento intersubjetivo correspondendo à **dignidade como construção social**, ou seja, resultado de reconhecimento mútuo, da proteção da **esfera comunicativa** (privacidade como condição para participação democrática) e da **integridade discursiva** (proteção contra manipulação informacional).

Framework para a proteção efetiva do “Brain Data Privacy”

1 Princípio da Neuroproteção Primária

Estabelecimento de presunção forte contra o processamento de dados neurais para finalidades não terapêuticas, invertendo o ônus da prova para demonstração de necessidade imperiosa.

2 Direito à Desconexão Neural

Reconhecimento do direito irrevogável de desconexão de qualquer interface neural, incluindo proteção contra pressões econômicas ou sociais para manutenção de conexões.

3 Proibição de Discriminação Neurocognitiva





Vedação de uso de dados neurais para discriminação em contextos de emprego, seguros, educação ou outros serviços essenciais.

4 Transparência Algorítmica Mandatória

Obrigação de explicabilidade completa de algoritmos que processam dados neurais.

O direito ao sonho emerge como resposta normativa à evolução de técnicas de manipulação onírica, como o Targeted Dream Incubation (TDI) e a Targeted Memory Reactivation (TMR). Experimentos recentes demonstram a possibilidade de inserir conteúdos específicos nos sonhos por meio de estímulos auditivos ou elétricos durante o sono REM.

Além dos riscos éticos, a manipulação de sonhos coloca em xeque o próprio conceito de liberdade psíquica, criando o risco de uma colonização do inconsciente por interesses comerciais, políticos ou ideológicos, a exemplo:

1. Manipulação Não Consentida: Tecnologias já existem para alterar conteúdo dos sonhos
2. Comercialização: Possível inserção de conteúdo publicitário durante o sono
3. Vigilância Onírica: Monitoramento de padrões de sonho para profiling psicológico
4. Alteração de Memória: TMR pode ser usado para fortalecer ou enfraquecer memórias específicas

A proposta de reconhecimento do direito ao sonho como direito fundamental se fundamenta em 4 pilares:

1. Proteção da Autonomia Psíquica: Garantia da liberdade mental mesmo durante estados inconscientes.
2. Proibição de Manipulação Onírica sem Consentimento – informado e destacado: Resguardando a inviolabilidade do espaço subjetivo do sonho.
3. Defesa da Integridade Cognitiva: Evitando interferências que alterem, condicionem ou explorem comercialmente o conteúdo onírico.





4. Direito à Continuidade Psicológica: A proteção da identidade pessoal contínua contra fragmentação ou alteração radical não voluntária da personalidade ou memória.

Esta proposta encontra respaldo normativo nos direitos fundamentais à intimidade e à vida privada, e na dignidade da pessoa humana/dignidade informacional, além de ser compatível com os desenvolvimentos mais recentes em neuroética (Lavazza, 2018).

A construção de um novo “Bill of Human Rights” para o século XXI exigirá esforço colaborativo entre múltiplos atores sociais, combinando expertise técnica com sabedoria jurídica e ética. O desafio não é apenas proteger contra os riscos emergentes, mas também garantir que as tecnologias sirvam ao florescimento humano e à dignidade de todas as pessoas.

O futuro dos direitos humanos e fundamentais está sendo escrito agora, nas decisões que tomamos sobre como regular e implementar essas tecnologias emergentes.

O direito ao sonho representa uma dimensão particularmente inovadora dos neurodireitos. À medida que as tecnologias de monitoramento neural se tornam capazes de acessar e interpretar a atividade cerebral durante o sono, torna-se essencial proteger este último refúgio da privacidade mental absoluta.

Este direito engloba múltiplas dimensões: o direito de sonhar sem interferência externa, a proteção contra a leitura ou gravação de sonhos, o direito ao esquecimento onírico, e a vedação da manipulação artificial dos conteúdos dos sonhos. O sonho representa o último território verdadeiramente privado da experiência humana, e sua proteção jurídica simboliza a resistência à colonização total da mente humana pela tecnologia. O direito ao sonho emerge como dimensão paradigmática da autonomia mental por representar a experiência mais íntima e irredutível da consciência humana. Os sonhos constituem domínio de pura subjetividade, não instrumentalizado por demandas externas e não direcionado para fins produtivos ou socialmente úteis.

Hannah Arendt identificou a vida contemplativa como esfera necessária para preservação da dignidade humana contra a invasão do social. Os sonhos representam a derradeira manifestação desta vida contemplativa: espaço mental completamente privado, não sujeito a escrutínio ou julgamento externo.



Há uma Dimensão Existencial do Sonhar, partindo do reconhecimento de Martin Heidegger ao enfatizar a importância do "ser-para-si" como condição da autenticidade existencial. O sonho constitui experiência paradigmática deste ser-para-si, livre das demandas do "ser-com-outros" e das estruturas sociais de significado.

O presente direito traz proteção específica em face de:

1. Decodificação de Conteúdo Onírico - Pesquisadores como Yukiyasu Kamitani no Japão já demonstraram capacidade de decodificar parcialmente conteúdo visual de sonhos através de fMRI. Embora ainda limitada, esta tecnologia projeta cenário onde sonhos poderão ser "lidos" diretamente.
2. Manipulação Onírica Comercial - Empresas já estariam desenvolvendo tecnologias para influência de conteúdo onírico, incluindo inserção de produtos comerciais em experiências oníricas.
3. Vigilância do Sono - Dispositivos de monitoramento do sono já coletam dados sobre padrões REM e atividade cerebral durante o sonho, criando "perfis oníricos" para fins comerciais.

Faz parte do conteúdo normativo do Direito ao Sonho:

1. Inviolabilidade Onírica

Proibição absoluta de acesso, monitoramento ou interferência em conteúdo onírico sem finalidade médica estritamente necessária e com salvaguardas excepcionais.

2. Não-Comercialização do Sonho

Vedação de uso comercial de dados oníricos ou inserção de conteúdo comercial em experiências oníricas.

3. Proteção contra Indução Onírica

Proibição de tecnologias que induzem sonhos específicos para fins não terapêuticos, preservando a espontaneidade onírica como dimensão da liberdade mental.

4. Direito ao Esquecimento Onírico

Garantia de que registros de atividade onírica sejam automaticamente deletados após finalidade médica, sem possibilidade de armazenamento ou processamento posterior.

4. Conceitos vagos e indeterminados trazendo insegurança jurídica





Há palavras no PL 2338 que geram insegurança jurídica pelo nível de abstração e indeterminação. É o que aponta a ANPD (https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-apresenta-propostas-de-alteracao-do-substitutivo-ao-pl-2338-sobre-inteligencia-artificial/Versao_final_07.05.24_PL_2338_Substitutivo_Comissao_Especial_Propostas_ANPD1.pdf) além do excesso de remissões a regulamentações futuras - excessiva delegação a regulamentos infralegais futuros (ex: "a autoridade competente definirá..."), o que pode comprometer a segurança jurídica e a previsibilidade. Deverá haver, pois atenção à vaguidade de conceitos tais como "autonomia humana", "tomada de decisão automatizada", e "intervenção humana significativa"; são termos considerados genéricos e carecem de definição normativa sólida. Outro conceito vago e indeterminado é o de "dano significativo" para considerar a IA de alto risco.

5. Omissões e lacunas

Alguns pontos críticos e de suma importância foram excepcionados do novo PL, em verdadeira omissão legislativa, sem fundamentação frente às evidências existentes de potencial de viés/bias, como no caso do reconhecimento facial, e da exclusão de aplicação da lei em aplicações quanto à defesa nacional. Neste âmbito, portanto, estariam legalizadas de forma ampla, irrestrita, sem qualquer accountability e medidas de mitigação o uso por exemplo de IA para fins de vigilância em massa, reconhecimento facial e captura de dados biométricos e para fins militares, onde se tem inclusive 2 agravantes maiores: risco de irreversibilidade da medida, com a morte ou lesão de pessoas, e impossibilidade de retorno ao "status quo ante", e autonomia da IA usada em contexto militar, dificultando o controle humano. Já há utilização de IA para fins militares como reports da ONU apontam sem quaisquer medidas de accountability, transparência e mitigação.

Como sugestão podemos citar a necessidade de substituir cláusulas genéricas (como "sistemas contrários ao interesse público") por listas objetivas, como no AI Act.





Os conceitos vagos do PL 2338 criariam insegurança, contudo, o AI ACT também contém conceitos abertos, como: “Uso inaceitável” (Art. 5); “Impacto significativo nos direitos fundamentais” (Art. 6); “Supervisão humana adequada” (Art. 14). Portanto, este não pode ser um critério para se justificar a afirmação de que o PL 2338 é mais forte na sua estrutura de obrigações do que o AI Act.

Entre omissões e lacunas que merecem revisão destacamos:

a) Reconhecimento Facial

- A nova versão legaliza o uso de reconhecimento facial, ainda que com requisitos condicionantes;
- Ineficácia para segurança pública;
- O PL original era mais protetivo ao prever uma espécie de moratória.

b) Exclusão da Defesa Nacional (art. 1º, parágrafo 1º)

- A proibição de armas letais autônomas (warfare AI) é esvaziada pela exclusão do escopo da lei quando se trata de defesa nacional;
- Uma vez que esse é justamente o contexto predominante de uso, a norma se torna inócuia.

c) O PL não traz proibição, portanto, de práticas em sistemas de IA incompatíveis com os direitos humanos tais como: como reconhecimento facial em espaços públicos e para fins de segurança nacional. Outrossim, seria importante complementar a proibição de classificação social: sistemas que avaliam ou classificam pessoas com base em seu comportamento social ou características pessoais, resultando em tratamento injusto ou discriminatório. No caso de identificação biométrica remota em tempo real em espaços públicos para aplicação da lei: Proibida, exceto em situações específicas, como busca por vítimas de crimes, prevenção de ameaças iminentes ou identificação de suspeitos de crimes graves, seria interessante acrescentar que são práticas autorizadas apenas mediante autorização judicial ou de autoridade competente. Ainda trazer a proibição de: criação de bancos de dados de reconhecimento facial por coleta indiscriminada de imagens: Sistemas que criam ou expandem bancos de dados de reconhecimento facial por meio da coleta indiscriminada de imagens de rostos de pessoas a partir da internet ou de imagens de câmeras de vigilância; inferência de emoções no local de trabalho ou em instituições de ensino: Sistemas que inferem emoções de indivíduos nesses





contextos, exceto quando justificados por razões médicas ou de segurança. Categorização biométrica para deduzir características sensíveis: Sistemas que categorizam pessoas com base em dados biométricos para deduzir ou inferir características como raça, opiniões políticas, convicções religiosas, orientação sexual, entre outras.

d) No tocante à categorização de risco, dispõe o artigo 12 que o próprio agente irá realizar avaliação preliminar do grau de risco, como boa prática, e segundo o § 2º caberá à autoridade setorial definir as hipóteses em que a avaliação preliminar será simplificada ou dispensada, observadas as normas gerais da autoridade competente. Não há justificativa alguma para dispensar tal análise ou simplificar a mesma em se tratando de risco alto, o que se pode é trazer incentivos tributários, e outras medidas para sustentar tal prática por startups e empresas de pequeno porte.

e) O artigo 6º. parágrafo 1º, traz uma interpretação não condizente com a teoria dos direitos fundamentais, e superável a uma interpretação sistemática e teleológica, sendo uma falha já da LGPD, qual seja, traz o respeito absoluto ao segredo comercial e industrial quando estes não são direitos absolutos, e podem ceder e ser flexibilizados diante do caso concreto, como dispõe a própria LPI ao prever salvaguardas a tal segredo: “§ 1º A explicação referida no inciso I do caput deste artigo, respeitado o segredo comercial e industrial, incluirá informações suficientes, adequadas e inteligíveis, nos termos de regulamento”.

f) O direito a supervisão humana no caso de alto risco também encontra uma ressalva nos termos: “A supervisão humana não será exigida caso sua implementação seja comprovadamente impossível ou implique esforço desproporcional, hipóteses em que o agente do sistema de IA de alto risco implementará medidas alternativas eficazes”. Melhor seria trazer o princípio da razoabilidade no caso e não da proporcionalidade, a exemplo, “mutatis mutandis” do disposto na LGPD para o caso de anonimização. Enquanto que a proporcionalidade estabelece um balanceamento entre meios e fins, a razoabilidade seria uma avaliação de viabilidade e pertinência prática frente as condições técnicas e fáticas, além disso, a **expressão “esforço desproporcional”** pode induzir a um **critério subjetivo ou arbitrário**, sem parâmetros claros de avaliação, bem como não



se refere diretamente à **capacidade técnica, econômica ou contextual**, como faz a LGPD ao usar **razoabilidade técnica** (art. 12, §2º). A expressão “razoabilidade” é **mais apropriada do que “proporcionalidade” no contexto técnico-regulatório do PL 2338/2023**, especialmente ao tratar de exceções a obrigações operacionais (como supervisão humana). Ela oferece um **critério mais objetivo, tecnicamente avaliável e juridicamente seguro**, em harmonia com a LGPD, o GDPR e o AI Act. Além disso o artigo 8º, parágrafo único do PL 2338 ao permitir que a supervisão humana não seja exigida caso ela seja “comprovadamente impossível ou implique esforço desproporcional” traz margem para exclusão de uma salvaguarda crítica em sistemas de alto risco, sem a exigência de contrapartidas rigorosas como previstas no AI Act. Isso contraria o princípio da precaução e o direito à supervisão humana prevista no GDPR (Art. 22) e no AI Act (Art. 14).

6. Previsão de lista de princípios pelo PL 2338

O PL 2338 segue uma estrutura principiológica, semelhante à da LGPD, que também usa conceitos como “boa-fé”, “razoabilidade”, “finalidade” — sem que isso tenha impedido sua aplicação, mas não se resume a uma lei principiológica, como era o caso do PL 2120. Ainda há uma cláusula de escape no PL ao prever regulamentação setorial posterior (Art. 60), o que permitirá calibragem prática, apesar de algumas falhas já apontadas.

Portanto, uma parte principiológica no PL é essencial desde que a lei não se resuma a isso como era o caso do PL 2120, e não pode ser desconsiderado o contexto do Sul Global e o papel dos princípios no direito brasileiro, portanto não há que se falar que o PL tem “sobrecarga principiológica”. A problemática não é trazer princípios protetivos os quais em geral são alias vagos e abstratos, mas trazer concretude a estes através de direitos expressos, boas práticas e compliance exigíveis de forma proporcional, a depender do nível de risco. Em países com déficit histórico de proteção institucional, a formulação principiológica garante margem de interpretação protetiva aos órgãos reguladores, o que não existe em modelos anglo-saxões. Além disso, o AI Act é baseado no modelo continental europeu, também principiológico e abstrato (vide uso do princípio da precaução no Art. 5). O modelo normativo brasileiro exige princípios para



garantir densidade constitucional e justiça intertemporal e social. A ausência de princípios robustos poderia enfraquecer a proteção.

7) Impacto ao meio ambiente

Ponto positivo - Inovação do projeto brasileiro em considerar questões ambientais se comparado com AI Act e com o PL 2120 que não trazem considerações acerca desta temática. O PL 2338/2023 incorpora a proteção ambiental como um de seus fundamentos, conforme o art. 2º, inciso IV, que estabelece a "proteção ao meio ambiente e ao desenvolvimento ecologicamente equilibrado" como princípio orientador. Essa diretriz visa assegurar que o desenvolvimento e a aplicação de sistemas de IA considerem a sustentabilidade ambiental. Em comparação, o AI Act da União Europeia não possui uma disposição específica sobre impacto ambiental, mas enfatiza a necessidade de sistemas de IA seguros e confiáveis, o que pode incluir considerações ambientais indiretas. No Reino Unido, embora não haja uma legislação específica sobre IA e meio ambiente, políticas públicas têm incentivado o desenvolvimento de tecnologias sustentáveis, alinhadas com metas de redução de emissões de carbono.

Ponto negativo – generalidade e abstração sem medidas concretas, nada fala de elaboração de análise de riscos diretos e indiretos ao meio ambiente, de elaboração de avaliação de impacto algorítmico, da criação de uma Agência e/ou observatório público voltado a tais objetivos, nem da necessidade de taxonomia de metodologia de avaliação de tais riscos e taxonomia mais clara de risco. Deverá trazer metas claras como a inclusão de métricas de impacto climático a partir da exigência de elaboração prévia de relatórios de impacto, incentivos fiscais e outros a modelos de IA energeticamente eficientes, e exigência de adoção prévia de tal instrumento e que traga medidas de mitigação obrigatórias.

O Projeto de Lei 2338/2023 estabelece princípios e diretrizes para o desenvolvimento, fomento e uso ético da IA com base na centralidade da pessoa humana.





Ponto positivo: centralidade humana e respeito, portanto, a valores indisponíveis embora não citados, mas que seriam uma decorrência lógica: dignidade humana e Estado Democrático de direito.

Ponto negativo: ainda poderia ser visto como uma abordagem antropocêntrica, já que não avança para o necessário “life planet AI”, ao invés de apenas “human centric AI”, vendo ainda o meio ambiente de forma limitada, como objeto a ser explorado e não como “natureza” e sujeito de direitos.

8) Medidas pró-inovação - Incentivos, políticas públicas e regime especial para startups

Embora as medidas em prol da inovação do PL sejam menos detalhadas e demandam mais concretude, a afirmação de ausência de fomento à inovação é incorreta. Falta implementação, não intenção normativa. O AI Act é extremamente rigoroso e detalhista para sistemas de alto risco, com: Avaliação ex ante obrigatória; Avaliação de conformidade com notified bodies (órgãos acreditados); Monitoramento contínuo; Obrigatoriedade de registro europeu e marcação CE Proibição de sistemas com pontuação social, manipulação subliminar e uso de reconhecimento facial em tempo real. O PL 2338, ao contrário, não tem órgão acreditador, nem estabelece mecanismos robustos de conformidade como no AI Act. O rigor no texto brasileiro decorre de cláusulas genéricas, mas a implementação prática é muito menos exigente do que o AI Act. Não se pode argumentar que há um obstáculo à inovação com o PI com base em uma leitura minimalista do AI Act, sem considerar a dureza real das obrigações técnicas e regulatórias da versão final do regulamento europeu.

Resta analisar, em suma, os seguintes pontos:

Traz obstáculos à inovação, especialmente em startups e pequenos negócios?;

Não traz mecanismos concretos de fomento, ao contrário do AI Act?

Quanto ao sandbox, ao passo que o AI Act (art. 53-54) cria sandboxes regulatórios obrigatórios, com isenções e apoio técnico para inovação, o PL não traz a obrigatoriedade apenas autoriza as autoridades setoriais a definir critérios diferenciados; menciona diretrizes vagas, sem estrutura de implementação nem



financiamento definido. Neste aspecto não tem mecanismos concretos e operacionais de fomento à inovação comparáveis aos da UE. O mesmo quanto a startups e pequenas empresas ao passo que o AI Act traz previsão clara de isenções e apoio técnico para startups (considerando impacto, usuários e recursos), o PL apenas menciona que “autoridades setoriais poderão criar critérios diferenciados” (Art. 67, par. único).

Portanto, há claros incentivos à inovação no PL como nos arts. 59 e 67, além de ser melhor operacionado em um sentido pelo menos se comparado com a lentidão da efetivação dos sandboxes no AI Act (que só serão operacionais em 2026). Deverá ser abordado o desequilíbrio de poder entre empresas e usuários no Brasil para se justificar que as obrigações do PL seriam excessivas para fornecedores, e não ignorar que a assimetria informacional, técnica e econômica no Brasil é ainda mais acentuada do que na Europa. O AI Act não propõe mecanismos compensatórios para proteção de grupos vulneráveis, como indígenas, população negra, crianças e idosos — temas previstos indiretamente no PL (arts. 3º e 5º). Fomentar inovação sem salvaguardas pode aumentar a exclusão digital e os danos estruturais.

O PI traz ainda no seu artigo 1º, parágrafo 2º casos de flexibilização de obrigações regulatórias previstas na Lei, a fim de promover o desenvolvimento tecnológico nacional. Em seu artigo 59, por sua vez, traz no parágrafo único medidas de fomento à inovação referidas no caput as quais serão pautadas por algumas diretrizes. Complementa tais disposições o art. 73. ao prever que com o fim de promover o desenvolvimento tecnológico nacional, o SIA regulamentará regimes simplificados, envolvendo flexibilização de obrigações regulatórias previstas nesta Lei em casos pontuais.

Apesar de, portanto, trazer diversos artigos com incentivos à inovação ainda há alguns pontos fracos do PL 2338 que destacamos:

1. Ausência de mecanismos operacionais claros

- As diretrizes não se traduzem em instrumentos vinculantes, como linhas de crédito específicas, agências executoras ou fundo nacional de IA, diferentemente da UE e Japão, que operam com programas já implementados.

2. Falta de definição para “critérios diferenciados”





- O art. 67, parágrafo único, exige que autoridades definam critérios diferenciados, mas não especifica os parâmetros, prazos ou formato, nem vincula isso a uma política de desenvolvimento.

3. Falta de métricas e indicadores de avaliação

- As diretrizes são amplas e não se vinculam a indicadores de desempenho, metas de inovação, ou mecanismos de accountability para as autoridades setoriais.

Propostas de Aperfeiçoamento

1. Criação de um Programa Nacional de Fomento à IA

- Institucionalizar um fundo específico, coordenado com FINEP, BNDES e CNPq, para apoiar desde P&D até a escalabilidade de soluções de IA.

2. Inclusão expressa de regras obrigatórias quanto ao regulatory sandboxes

- Estabelecer bases legais e princípios para sandbox regulatório multissetorial, com adesão voluntária, supervisionada por uma autoridade coordenadora nacional (como ocorre na França e no Reino Unido) e dispor acerca da ausência de sanções não como opção como está agora.

3. Metas e indicadores de inovação

- O art. 59 poderia trazer metas de: número de empresas beneficiadas, patentes nacionais, uso de IA em serviços públicos, internacionalização de startups brasileiras, etc.

4. Tratamento diferenciado orientado por riscos

- Estabelecer que os critérios diferenciados para startups considerem risco do sistema, maturidade do mercado e capacidade técnica, e não apenas “número de usuários” (como prevê o art. 67 atual).

5. Capilaridade federativa

- A diretriz de inovação deve prever mecanismos de regionalização da inovação em IA, com polos estaduais, conectando o Brasil profundo à IA, como ocorre na Espanha com o *AI Digital Innovation Hubs*.

Medidas em Prol da Inovação – previsão e implementação prática

O PL 2338 especialmente no art. 3º e nos capítulos sobre políticas públicas e fomento traz diretrizes gerais como:





Iniciativas Legislativas

- Regime especial para startups e pequenas empresas (não detalhado).
- Incentivos fiscais para desenvolvimento de IA responsável (sem instrumentos definidos).
- Parcerias público-privadas (conceito amplo).

Políticas Públicas

- Criação de programas de capacitação em IA.
- Fomento à pesquisa e desenvolvimento - P&D.
- Estabelecimento de centros de excelência em IA

O artigo 15 do PL estabelece diretrizes para políticas públicas de fomento à inovação, determinando que o poder público deve promover o desenvolvimento da IA nacional através de incentivos específicos.

Crítica: previsões são genéricas e não vinculantes

- Não há previsão de instrumentos orçamentários ou regulatórios específicos.
- Falta de prazos, metas, responsáveis e formas de implementação.
- Ausência de indicadores de avaliação de impacto ou de fundos públicos dedicados.

Sandbox Regulatório

Embora o PL preveja a implementação de ambientes regulatórios experimentais (sandboxes) (art. 55 § 2º) para permitir o teste de sistemas de IA em condições controladas, trazemos as seguintes sugestões.

Sugestão: o PL não dispõe se haverá suspensão de sanção durante o período, não traz definição de limites claros para esses ambientes; não há garantias de que haverá respeito pelos direitos básicos daqueles afetados, nada se fala de respeito a LGPD, consentimento informado, e incluir avaliação de impacto antes de qualquer teste com humanos; falta, pois, tornar o sandbox regulatório mais funcional, estabelecer critérios claros para adesão, limites temporais, supervisão e garantias de direitos fundamentais durante os testes com IA, reforçar o papel da autoridade coordenadora com expertise técnica em IA:



Ao invés de delegar integralmente a reguladores setoriais que podem não ter familiaridade técnica com IA (como no modelo britânico), o Brasil pode adotar um modelo misto:

- Uma autoridade nacional especializada em IA, com caráter técnico e transversal (como uma "Agência Nacional de Inteligência Artificial");
- Suporte técnico às agências setoriais, mediante diretrizes vinculantes e compartilhamento de recursos.

Comparação com AI Act: O AI Act estabelece sandboxes regulatórios no artigo 57, exigindo que cada Estado-membro estabeleça pelo menos um sandbox até agosto de 2026. O modelo brasileiro apresenta maior flexibilidade na definição de critérios de entrada.

Reino Unido: A abordagem britânica enfatiza sandboxes setoriais, com reguladores específicos supervisionando a experimentação em suas áreas de competência.

Como poderiam ser implementadas na prática?

1. Regime especial para startups

Como implementar:

- Adotar um marco legal complementar (ex: Estatuto da IA Inovadora).
- Criar uma categoria de “agente de IA emergente” com:
 - Redução proporcional de exigências;
 - Apoio técnico e jurídico na conformidade.

Referência: modelo da França (AI Startups Fast-Track) e UK AI Foundry.

2. Incentivos fiscais

Como implementar:

- Leis complementares ao PL (como via Lei do Bem ou Lei da Inovação);
- Dedutibilidade acelerada para investimentos em IA ética, explainable AI, ESG-IA.

Referência: regime japonês de crédito fiscal para tecnologias emergentes sustentáveis.

3. Parcerias público-privadas

Como implementar:

- Editais coordenados entre BNDES, Finep, MCTI e empresas.
- Modelos de sandbox colaborativo regulado (modelo Estônia + Reino Unido).





4. Programas de capacitação

Como implementar:

- Currículos nacionais em IA no ensino técnico e superior (via MEC e CAPES);
- Bolsas de inovação IA para minorias (ex: mulheres negras em IA, comunidades indígenas digitais);
- Integração com a Estratégia Brasileira de IA (EBIA) e o PBIA.

5. Centros de excelência

Como implementar:

- Convênios federais com universidades federais, ICTs, SENAI e hubs estaduais.
- Avaliação por mérito técnico e impacto social.
- Requisitos de pesquisa aberta e ética algorítmica.

Colaboração público-privada

A colaboração entre os setores público e privado, conforme mencionada no PL 2338/2023, refere-se à parceria entre órgãos governamentais e empresas privadas para o desenvolvimento, implementação e supervisão de tecnologias de IA. Contudo seria necessário criar mecanismos claros e concretos de se criar tais colaborações, pois na prática diversos empecilhos e obstáculos impedem sua efetivação.

Ainda no tocante a temática da inovação, merecem atenção as novas propostas da UE de 2025 (Pacto para IA, Código de Conduta, Painel Científico). Essas iniciativas — o *AI Act Service Desk* e o plano *AI Continent* — revelando uma inflexão da Comissão Europeia para uma **abordagem equilibrada**, na qual a **inovação é vista como aliada da regulação**, e não sua vítima; percebe-se, pois, que a **implementação do AI Act é acompanhada de políticas públicas de apoio**, especialmente para pequenas empresas e agentes não estatais; o ecossistema de IA é pensado de forma **multidimensional**, combinando aspectos técnicos, éticos, sociais, econômicos e ambientais. A proposta representa um importante instrumento de governança responsável, ou seja, um mecanismo público de mediação entre inovação tecnológica e a densidade regulatória. Funciona como uma ponte entre o regulador e o ecossistema inovador, promovendo um ambiente regulatório mais compreensível e, portanto, mais favorável ao desenvolvimento de IA responsável. A EU portanto, traz a ênfase em inovação



responsável, reconhecendo que excessiva rigidez regulatória pode sufocar o potencial de inovação e, por isso, articula instrumentos de mitigação de risco que não inibem a criatividade tecnológica, mas garantem responsabilidade.

A proposta serve como instrumento complementar ao AI Act, funcionando como a dimensão prática e política do que a legislação técnica estabelece, favorecendo um ambiente de confiança mútua entre o setor privado, academia e órgãos públicos.

Essas duas iniciativas — o *AI Act Service Desk* e o plano *AI Continent* — revelam uma inflexão da Comissão Europeia para uma abordagem equilibrada, na qual:

- A inovação é vista como aliada da regulação, e não sua vítima;
- A implementação do AI Act é acompanhada de políticas públicas de apoio, especialmente para pequenas empresas e agentes não estatais;
- O ecossistema de IA é pensado de forma multidimensional, combinando aspectos técnicos, éticos, sociais, econômicos e ambientais.

7) Avaliação de impacto algorítmico - AIA obrigatória para sistemas de alto risco

Ponto positivo: o PL traz a temática da elaboração de avaliação de impacto para alto risco, ausente no PL 2120 e criação de base pública de sistemas de IA.

Ponto negativo: não traz requisitos do conteúdo e proceduralização para elaboração da AIA, requisitos para quem elabora (institutos e organismos independentes, multistakeholder, com inclusão, abordagem co-approach – participação de representantes de comunidades afetadas, e grupos vulneráveis; não especifica que deverá ser elaborado de forma prévia (antes da ocorrência do dano, antes de colocar no mercado a aplicação da IA – ex. Caso genocídio Myanmar x Facebook) – razão de ser do instituto jurídico – interpretação sistemática e funcional e não literal, grammatical. Assim caímos no mesmo problema da Lgpd quanto ao RIPP – Relatório de Impacto a proteção de dados, trazendo insegurança jurídica devido à má técnica legislativa, já que não é clara quanto a ser um documento obrigatório, e como deverá ser elaborado e quando. Embora o artigo 2, XIV preveja a proteção e promoção de grupos vulneráveis não vai além disso, salvo a recomendação do artigo 5º, § 2º ao afirmar que os sistemas de IA que se destinem a grupos vulneráveis deverão, em todas as etapas de seu ciclo de vida,



ser transparentes e adotar linguagem simples, clara e apropriada à idade e à capacidade cognitiva, e ser implementados considerando o melhor interesse desses grupos. Não traz o PL abordagem inclusiva e democrática (coaprouch) que vai além e é um complemento da abordagem multistakeholder, devendo exigir consulta pública e envolvimento de grupos vulneráveis nas avaliações e em órgãos de revisão; há, pois, falta de participação popular e controle democrático não trazendo mecanismos de participação cidadã, controle social ou consulta pública obrigatória.

8) Responsabilidade Jurídica (AI Liability Directive vs. PL 2338)

Embora afirme que nas relações de consumo se aplica o CDC, não define se a responsabilidade é objetiva ou subjetiva, gerando insegurança jurídica.

Além disso poderia trazer 2 mecanismos extras a considerar o alto risco da IA e o porte econômico da empresa envolvida, quais seja seeguro obrigatório e fundo complementar compensatório para facilitar a indenização em termos reparatórios à vítima como é previsto pela UE em alguns documentos.

Neste sentido destacam-se as seguintes fontes:

- **AI Liability Directive (Diretiva de Responsabilidade Civil por IA) ao prever a presunção de causalidade**, quando o fornecedor ou operador descumprir obrigações estabelecidas no *AI Act* (ex: falta de AIA, falha na transparência), presume-se que isso contribuiu para o dano.
- **Revisão da Diretiva sobre Responsabilidade do Produto (Product Liability Directive - PLD) - <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0495>** trazendo a responsabilidade **objetiva** do fabricante (independentemente de culpa) por danos causados por IA defeituosa. Há previsão ainda de possibilidade de **exigir** dos operadores ou fabricantes “garantias financeiras apropriadas”, como seguros e aponta para uma possível existência de **fundos de compensação nacionais**, sobretudo para sistemas de **alto risco** e IA autônoma.
- **European Parliament Resolution on Civil Liability for AI (2020/2014(INL)) - https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_EN.html** -

Propôs criação de:

- Seguro obrigatório para sistemas de **IA de alto risco**;





- **Fundo de compensação da UE** em casos de desenvolvedores sem solvência.

CONSIDERAÇÕES FINAIS

A questão do que obsta ou maximiza a inovação vai além de análises simplistas, pois envolve diversos temas além de qual conteúdo estaria presente na lei, ou seja, uma lei que estabeleça obrigações proporcionais ao risco e que também preveja incentivos e/ou regime diferenciado para startups e microempresas, medidas pró inovação com o sandbox e acrescido de políticas públicas reais e concretas não irá obstar a inovação.

Aliás o entendimento da EU é no sentido de que a regulação é medida em prol da inovação. O PL 2338 acerta ao reconhecer a necessidade de políticas de fomento e tratamento diferenciado, mas ainda carece de mecanismos normativos, programáticos e institucionais concretos para que as medidas sejam aplicáveis e eficazes.

A comparação com o AI Act, modelo britânico e japonês mostra que, apesar de o Brasil estar no caminho certo em termos de diretrizes, falta musculatura executiva e articulação com políticas públicas existentes para que startups e inovação em IA realmente floresçam com competitividade global. O PL não cita isenções fiscais ou redução de taxas específicas, ao contrário do UK AI Regulation White Paper (2023) (Sugere incentivos em ambientes de testes, sem medidas fiscais) e do Ai Strategy do Japão de 2019 e atualizada em 2022 (Estratégia propõe subsídios e incentivos fiscais, mas sem artigo de lei específico). **O PL 2338 apresenta uma boa formulação principiológica, mas poucas medidas executivas concretas** (sem isenção de tributos, fundos dedicados, mecanismos automáticos de apoio técnico ou financeiro). Como pontos positivos destaca-se o fato de o PL 2338/2023 prever a promoção da inovação responsável como um de seus objetivos centrais, i.e, a inovação não é vista como um fim em si mesmo, e conjuga-se com isso à ética (metainovação – Floridi) e com a responsabilidade (Art. 1º). O Art. 3º estabelece diretrizes para políticas públicas que incentivem a pesquisa e o desenvolvimento em IA, incluindo a criação de ambientes propícios à experimentação e à colaboração entre setores público e privado. Há, pois, certa articulação entre regulação e políticas públicas, trazendo menção a tais questões e



trazendo deveres estatais como investimento em pesquisa e soberania tecnológica, além do estímulo a padrões interoperáveis.

Ainda quanto a startups dispõe como medida de Incentivo a Microempresas, Empresas de Pequeno Porte e Startups em seu art. 67 que as autoridades setoriais deverão definir critérios diferenciados para sistemas de IA ofertados por microempresas, empresas de pequeno porte e startups que promovam o desenvolvimento da indústria tecnológica nacional. Parágrafo único. Critérios diferenciados devem considerar o impacto concorrencial das atividades econômicas correlatas, o número de usuários afetados e a natureza das atividades econômicas exercidas.

Contudo, os avanços são tímidos se comparados com a EU/UK.

Na União Europeia, o AI Act inclui medidas de apoio à inovação, como a criação de sandboxes regulatórios (Art. 57) e programas de financiamento para projetos de IA. Recentemente, a UE lançou a iniciativa "Apply AI Strategy", visando acelerar a adoção de IA e impulsionar a inovação no continente (artificialintelligenceact.eu, joint-research-centre.ec.europa.eu).

O Reino Unido, por sua vez, adotou uma abordagem pro-inovação em sua estratégia regulatória para IA, conforme delineado no "AI Regulation: A Pro-Innovation Approach". Tais iniciativas precisam ser estudadas para se complementar as medidas a favor da inovação do PL 2338.

O art. 3º do PL 2338/2023 estabelece diretrizes para políticas públicas que incentivem a pesquisa e o desenvolvimento em inteligência artificial (IA), incluindo a criação de ambientes propícios à experimentação e à colaboração entre setores público e privado.

Sugestões adicionais complementares: incentivar o uso de IA para o fim da promoção do desenvolvimento sustentável, redução das desigualdades e inclusão social. Trazer medidas concretas e metas para o fomento à capacitação e à formação de recursos humanos, desde o ensino básico até a pós-graduação. Criação de mecanismos de governança e supervisão, como Oversight Board independente e público, agência de auditorias públicas. Assegurar que a promoção da transparência e explicabilidade se voltem aos usuários finais, permitindo a contestabilidade e a auditabilidade.



REFERÊNCIAS

ACEMOGLU, Daron; JOHNSON, Simon. Power and progress: our thousand- year struggle over technology and prosperity. New York: PublicAffairs, 2023. AIZENBERG, Evgeni; VAN DEN HOVEN, Jeroen. Designing for human rights in AI. *Big Data & Society*. Disponível em: <https://arxiv.org/abs/2005.04949>.

ALLEN, Danielle. *Justice by means of democracy*. Chicago: University of Chicago Press, 2023.

ALMEIDA, Virgílio; DONEDA, Danilo; GASSER, Urs. A layered model for AI governance. *IEEE Internet Computing*, v. 21, n. 6, p. 58–62, 2017.

ALMEIDA, Virgílio; MENDONÇA, Ricardo Fabrino; FILGUEIRAS, Fernando. Algorithmic institutionalism: the changing rules of social and political life. Oxford: Oxford University Press, 2014.

AYRES, Ian; BRAITHWAITE, John. *Responsive regulation: transcending the deregulation debate*. Oxford: Oxford University Press, 1992. Disponível em: <http://johnbraithwaite.com/wp-content/uploads/2016/06/Responsive-Regulation-Transce.pdf>.

BAROCAS, Solon; HOOD, Sophie; ZIEWITZ, Malte. Governing algorithms: a provocation piece. Paper preparado para a Governing Algorithms Conference, p. 1-12, 2013. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2245322.

BENJAMIN, Ruha. *Race after technology: abolitionist tools for the new Jim Code*. Cambridge: Polity Press, 2019.

BERMAN, Paul Schiff. Cyberspace and the state action debate: the cultural value of applying constitutional norms to “private” regulation. *University of Colorado Law Review*, v. 71, p. 1263–1310, 2005. Disponível em: https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=1083&context=faculty_publications.

BOAVENTURA DE SOUSA SANTOS. *A difícil democracia: reinventar as esquerdas*. São Paulo: Boitempo, 2021.

BRUNO, Fernanda (Coord.). *Tecnopolíticas da vigilância: perspectivas da margem*. São Paulo: Boitempo, 2018.

BURRELL, Jenna. How the machine ‘thinks’: understanding opacity in machine learning algorithms. *Big Data & Society*, 2016. Disponível em: <https://journals.sagepub.com/doi/full/10.1177/2053951715622512>.

CAMPBELL-VERDUYN, Malcolm; GOGUEN, Miles; PORTER, Tony. Big data and algorithmic governance: the case of financial practices. *New Political Economy*, v. 22, n. 2, p. 219, 2017. Disponível em: <https://www.researchgate.net/publication/306034022>.





CANTARINI, Paola; GUERRA FILHO, Willis S. Teoria inclusiva dos direitos fundamentais e direito digital. São Paulo: Clube de Autores, 2020.

CANTARINI, Paola. Artificial Intelligence: regulatory challenges and riskification. *Revista Jurídica Unicuritiba*, v. 5, n. 67, p. 136–149, 2021. Disponível em: <http://revista.unicuritiba.edu.br/index.php/RevJur/article/view/5626/pdf>.

CANTARINI, Paola. Biopolítica digital e novas formas de racismo em tempos de crise autoimunitária. *Public Interest Journal*, Belo Horizonte, v. 22, n. 122, p. 45–65, 2020. Disponível em: <https://dspace.almg.gov.br/handle/11037/38536>.

CANTARINI, Paola. Governança de algoritmos de IA – uma abordagem das epistemologias do Sul. *Unicuritiba Journal*, v. 5, n. 72, p. 393–423, 2022. Disponível em: <http://revista.unicuritiba.edu.br/index.php/RevJur/article/view/6286>.

CANTARINI, Paola. IA, direitos fundamentais por design e Estado Democrático de Direito desde a concepção. *Revista Jurídica Unicuritiba*, v. 4, n. 76, p. 22– 45, 2023. Disponível em: <https://revista.unicuritiba.edu.br/index.php/RevJur/article/view/6681>.

CANTARINI, Paola. Filosofia da AI, Lumen Juris editora, 2023.

CANTARINI, Paola. Governança da IA, Lumen Juris editora, 2024.

CHEHOUDI, Rafaia. Artificial intelligence and democracy: pathway to progress or decline. Journal of Information Technology & Politics, 2025.

CHOMSKY, Noam. Surviving the 21st century. New York: Penguin Books, 2021.

CHUL HAN, Byung. A sociedade da transparência. Petrópolis: Vozes, 2017.

CIHON, Peter. Standards for AI governance: international standards to enable global coordination in AI research & development. Oxford: Future of Humanity Institute, 2019.

CIHON, Peter; MAAS, Matthijs M.; KEMP, Luke. Should artificial intelligence governance be centralised? Design lessons from history. In: Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society (AIES), New York, 2020.

COECKELBERGH, Mark. Why AI undermines democracy and what to do about it. Cambridge: Polity Press, 2024.

COUNCIL OF EUROPE. Framework convention on AI and human rights. Strasbourg, 2024.





CRAWFORD, Kate. *Atlas of AI: power, politics, and the planetary costs of artificial intelligence*. New Haven: Yale University Press, 2021.

DAFOE, Allan. *AI governance: a research agenda*. Oxford: Future of Humanity Institute, 2018.

DAFOE, Allan. *AI governance: opportunity and theory of impact*. 2020. Disponível em: <https://www.allandafoe.com/opportunity>.

DATA & SOCIETY. *Algorithmic accountability: a primer*. New York, 2018. Disponível em: https://datasociety.net/wp-content/uploads/2018/04/Data_Society_Algorithmic_Accountability_Primer_FIN_AL-4.pdf.

DONEDA, Danilo; ALMEIDA, Virgílio. *What is algorithm governance?* IEEE Internet Computing, v. 20, n. 4, p. 60–63, 2016.

EUBANKS, Virginia. *Automating inequality: how high-tech tools profile, police, and punish the poor*. New York: St. Martin's Press, 2018.

FLORIDI, Luciano. *The ethics of information*. Oxford: Oxford University Press, 2013.

FLORIDI, Luciano. *The fourth revolution: how the infosphere is reshaping human reality*. Oxford: Oxford University Press, 2014.

FLORIDI, Luciano. *The onlife manifesto: being human in a hyperconnected era*. Cham: Springer, 2015.

GASSER, Urs; ALMEIDA, Virgílio. *A layered model for AI governance*. IEEE Internet Computing, v. 21, n. 6, p. 58–62, 2017.

GOOGLE. *Perspectives on issues in AI governance*. Disponível em: [\[https://ai.google/static/documents/perspectives-on-issues-in-ai-governance.pdf\]](https://ai.google/static/documents/perspectives-on-issues-in-ai-governance.pdf) (<https://ai.google/static/documents/perspectives-on-issues-in-ai-governance.pdf>).

HOFFMANN-RIEM, Wolfgang. *Teoria geral do direito digital*. Rio de Janeiro: Forense, 2022.

HOOD, Christopher; HOTHSTEIN, Henry; BALDWIN, Robert. *Government of risk: understanding risk regulation regimes*. Oxford: Oxford University Press, 2001.

HUÉRFANO, Eliana Herrera; CABALLERO, Francisco Sierra; ROJAS, Carlos Del Valle. *Hacia una epistemología del Sur: decolonialidad del saber-poder informativo*. Disponível em: [\[https://dialnet.unirioja.es/servlet/articulo?codigo=5792037\]](https://dialnet.unirioja.es/servlet/articulo?codigo=5792037) (<https://dialnet.unirioja.es/servlet/articulo?codigo=5792037>).



KALPOKAS, Ignas. Algorithmic governance: politics and law in the post-human era. London: Palgrave Pivot, 2019.

KROLL, Joshua. Accountable algorithms. 2015. Disponível em: [\[https://www.jkroll.com/papers/dissertation.pdf\]](https://www.jkroll.com/papers/dissertation.pdf)

LOTINGER, Sylvère; VIRILIO, Paul. The accident of art. New York: Semiotext(e), 2005.

MOROZOV, Evgeny. Silicon Valley: i signori del silicio. Milano: Codice Edizioni, 2019.