

CONTRIBUIÇÕES À COMISSÃO ESPECIAL DE
INTELIGÊNCIA ARTIFICIAL DA CÂMARA DOS
DEPUTADOS: **PL 2338/2023**

Setembro de 2025

SOBRE A DATA PRIVACY BRASIL

A Data Privacy Brasil é uma organização que nasce da união entre uma escola e uma associação civil em prol da promoção da cultura de proteção de dados e direitos digitais no Brasil e no mundo.

Fundada em 2018, a Data Privacy Brasil Ensino surge como um espaço para difundir e inovar no conhecimento sobre privacidade e proteção de dados no país. Com conteúdo adaptado para uma linguagem mais prática, com exercícios e estudos de caso, esta é uma escola para todos aqueles que se interessam e querem se aprofundar na rica temática da privacidade, proteção de dados e novas tecnologias.

A Associação Data Privacy Brasil de Pesquisa é uma organização da sociedade civil, sem fins lucrativos e suprapartidária, que promove a proteção de dados pessoais e outros direitos fundamentais a partir de uma perspectiva da justiça social e assimetrias de poder.

A partir de 2023, as duas instituições se unem para formar uma única organização, mantendo os mesmos princípios e atividades. Com o apoio de uma equipe multidisciplinar, realizamos formações, eventos, certificações, consultorias, conteúdos multimídia, pesquisas de interesse público e auditorias cívicas para promoção de direitos em uma sociedade datificada marcada por assimetrias e injustiças. Por meio da educação, da sensibilização e da mobilização da sociedade, almejamos uma sociedade democrática onde as tecnologias estejam à serviço da autonomia e dignidade das pessoas.

www.dataprivacy.com.br | www.dataprivacybr.org

DIREÇÃO

Bruno Bioni, Mariana Rielli e Rafael Zanatta

COORDENAÇÃO

Carla Rodrigues, Jaqueline Pigatto, Pedro Martins, Pedro Saliba e Victor Barcellos

EQUIPE

Barbara Yamasaki, Bianca Marques, Eduardo Mendonça, Gabriela Vergili, Giovana Andrade, Isabelle Santos, Johanna Monagreda, João Paulo Vicente, Larissa Pacheco, Louise Karczeski, Luíze Ribeiro, Matheus Arcanjo, Natasha Nóvoa, Pedro Henrique, Rafael Guimarães, Rennan Willian, Rodolfo Rodrigues e Vinicius Silva.

LICENÇA

Creative Commons

É livre a utilização, circulação, ampliação e produção de documentos derivados desde que citada a fonte original e para finalidades não comerciais.

IMPRENSA

Para esclarecimentos sobre o documento e entrevistas, entrar em contato pelo e-mail imprensa@dataprivacybr.org

Índice

Introdução	6
TÓPICOS	7
01. DISPOSIÇÕES PRELIMINARES E DEFINIÇÕES	9
02. DOS DIREITOS FUNDAMENTAIS	15
03. CLASSIFICAÇÃO E CATEGORIAS DE RISCO	25
04. AVALIAÇÕES DE IMPACTO ALGORÍTMICO	28
05. BOAS PRÁTICAS E GOVERNANÇA	36
06. SISTEMA NACIONAL DE REGULAÇÃO E GOVERNANÇA (SIA)	41
07. ATUAÇÃO DO PODER PÚBLICO	62
Sugestões de leituras complementares	73

INTRODUÇÃO

A Data Privacy Brasil oferece neste texto contribuições propositivas para melhoria da redação jurídica do Projeto de Lei 2338/2023. As contribuições foram elaboradas a partir de um esforço coletivo do time de pesquisadores da organização, que reúne profissionais do direito, ciência política, ciências da comunicação, relações internacionais, sociologia e economia política.

Considerando que o público-alvo é formado por assessores parlamentares da Comissão Especial de Inteligência Artificial da Câmara dos Deputados, a linguagem é propositiva e fundamentada em uma metodologia de justificativa e proposição. Assim, para cada capítulo do projeto de lei que consideramos relevante, identificamos melhorias específicas no texto de lei, que identificamos com a cor vermelha.

As referências acadêmicas e de suporte para as justificativas estão incluídas em hiperlinks, evitando uma linguagem acadêmica excessivamente rebuscada no teor do texto. Sempre que possível, buscamos referências em documentos do sistema internacional de direitos humanos, incluindo o Pacto Digital Global, e em documentos oficiais do G20, do T20 e de documentos governamentais sobre Inteligência Artificial.

As contribuições também refletem a missão institucional da Data de promoção de um ecossistema informacional justo e a defesa incondicional de direitos fundamentais, que são conciliáveis com uma abordagem de fomento à ciência, à pesquisa e à inovação tecnológica.

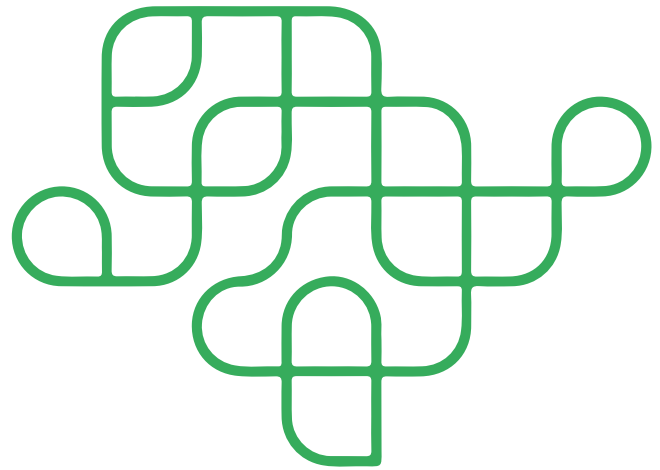
As propostas sobre interoperabilidade, governança de dados e ecossistema de dados foram produzidas em parceria com o Instituto de Direito de Público (IDP), por meio de esforço conjunto de pesquisa acadêmica. Confira nossa contribuição conjunta no QR Code abaixo!



TÓPICOS

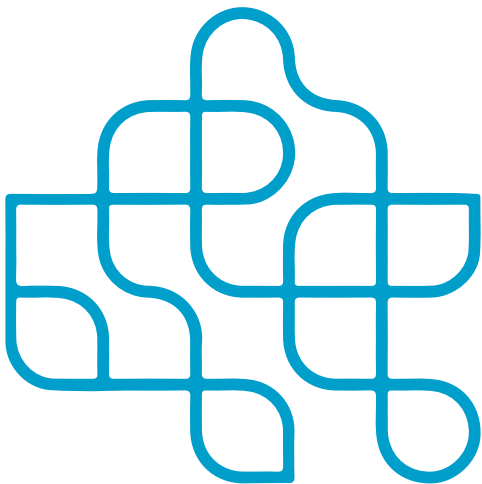
- **Atualização das disposições preliminares**
- **Dos direitos fundamentais**
- **Do Alto Risco**
- **Procedimentalização de avaliações de impacto algorítmico e retirar poderes normativos de autoridades setoriais sobre a procedimentalização da AIA**
- **Código de conduta e interoperabilidade de dados**
- **ANPD, autoridades setoriais, aspectos concorrenciais, e multissetorialismo**
- **Governança de dados, segurança nacional, segurança pública, e sustentabilidade**





01.

DISPOSIÇÕES PRELIMINARES E DEFINIÇÕES



01. DISPOSIÇÕES PRELIMINARES E DEFINIÇÕES

Escopo de aplicação e exceção

JUSTIFICATIVA

Ainda que as aplicações de IA voltadas para a defesa nacional devam ter objetivos específicos, assim como regime jurídico próprio, é importante trazer balizas de modo que seu desenvolvimento não seja irrestrito, com riscos de violações sem a devida responsabilização. Nesse sentido, a proposta é alinhar a redação atual à Lei Geral de Proteção de Dados: em seu artigo 4º, III, há também exceção de aplicabilidade da legislação à defesa nacional, com observação ao devido processo legal, princípios e direitos de titular de dados.

Com vistas à harmonização legislativa e aderência aos preceitos constitucionais, propõe-se a adição de texto semelhante, adequado às propostas da regulação de IA no país.

REDAÇÃO ATUAL

§ 1º Esta Lei não se aplica ao sistema de IA:

(...)

II – desenvolvido e utilizado única e exclusivamente para fins de defesa nacional;

PROPOSTA

§ 1º Esta Lei não se aplica ao sistema de IA:

(...)

II – desenvolvido e utilizado única e exclusivamente para fins de defesa nacional, observados o devido processo legal, princípios e fundamentos previstos nesta lei.

Grupo vulnerável

JUSTIFICATIVA

A lei oferece um conceito de vulnerabilidade, mas não de grupo vulnerável, que é a expressão mais usada na proposta de texto legal. A falta de definição legal pode acarretar problemas interpretativos da Lei de IA.

A definição proposta inspira-se no AI Act, que possui um enfoque em normas proibitivas sobre sistemas de IA que exploram as vulnerabilidades de uma pessoa ou de um grupo específico de pessoas devido à sua idade, deficiência ou situação social ou econômica específica.

Ao contrário de indivíduos que, ao menos em tese, dispõem de plenas condições de análise crítica e de acesso a recursos de proteção dos seus próprios direitos e interesses, os grupos vulneráveis podem ter menor capacidade de avaliar riscos, identificar manipulações ou reagir a injustiças produzidas por sistemas automatizados. Isso significa que os impactos negativos da inteligência artificial tendem a ser mais intensos e desproporcionais sobre essas populações.

A inclusão expressa desse conceito em norma jurídica é, portanto, indispensável. Ele oferece parâmetros normativos para que o Poder Público e os agentes regulados possam formular políticas de mitigação de riscos, mecanismos de transparência e salvaguardas adequadas. Além disso, alinha-se a princípios constitucionais como a dignidade da pessoa humana, a igualdade material e a proteção de direitos fundamentais, assegurando que a inovação tecnológica não aprofunde desigualdades já existentes.

REDAÇÃO ATUAL

Art. 4º Para os fins desta Lei, adotam-se as seguintes definições:

(...)

PROPOSTA

Art. 4º Para os fins desta Lei, adotam-se as seguintes definições:

(...)

XXXI - grupo vulnerável: conjunto de pessoas naturais que, devido a características específicas, como condições cognitivas, sociais, étnico-raciais, econômicas e etárias, a exemplo de crianças e adolescentes, idosos e pessoas com deficiência, estão em maior risco de serem desproporcionalmente afetadas pelos impactos negativos, falhas ou vieses de sistemas de inteligência artificial.

Atualização das disposições preliminares

JUSTIFICATIVA

Os temas de governança de dados e interoperabilidade devem ser objetos de leis específicas, não cabendo a essa lei esgotar a questão, mas combiná-las com IA por serem elementos estruturantes de uma governança mais holística. Um exemplo é o Marco Civil da Internet, com normas de proteção de dados pessoais que posteriormente influenciou a Lei Geral de Proteção de Dados Pessoais. Como os sistemas de IA dependem diretamente de dados para seu funcionamento, e principalmente de dados de qualidade, com diversidade e origem ética, é necessário estabelecer como base fundacional uma política de governança de dados. Documentos como o Pacto Global Digital da ONU (ver Objetivo 4) reconhecem a centralidade dessa governança para promover a inovação, os direitos humanos e os Objetivos de Desenvolvimento Sustentável (ODS). Nota-se, portanto, que o cenário internacional começa a avançar uma abordagem de “governança de dados social”, que abrange tanto os processos de gestão de dados como fatores sociais, políticos e econômicos (ver definição de social data governance do texto “Social data governance: Towards a definition and model” na p.3).

O reconhecimento da dimensão social da governança de dados visa garantir transparência, responsabilidade e respeito aos direitos fundamentais, como privacidade, não discriminação, e equidade. Políticas de governança de dados, portanto, são fundamentais para o controle sobre ambos o ciclo de vida de sistemas de IA, relacionado aos processos de desenvolvimento e aplicação dessas tecnologias, e o ciclo de vida dos dados, referente ao tratamento dos dados que alimentam esses sistemas, enquanto processos dependentes mas distintos. Esse controle ajuda a prevenir vieses, abusos e impactos negativos, especialmente sobre grupos vulneráveis, o que é essencial para se estabelecer uma IA confiável e alinhada ao interesse público.

Ainda, a adoção de políticas alinhadas a uma “governança de dados social” funciona como garantia para o desenvolvimento de sistemas de IA que promovam a livre iniciativa e o mercado interno, observando a soberania nacional e o desenvolvimento cultural, socioeconômico e bem-estar da população (vide art. 170 e art. 219 da Constituição Federal). Estabelecer tais políticas, portanto, é fundamental para promover um ecossistema informacional justo, ou seja, reconhecer de forma holística as intersecções entre tecnologia e sociedade de forma que previna os riscos e amplie os benefícios da transformação digital.

Essas questões já estão bem sinalizadas em documentos de nível internacional que baseiam estas contribuições. A presente definição de governança de dados é inspirada na Minuta da Política de Governança e Compartilhamento de Dados (ver art.2º) do governo federal (objeto de consulta pública atualmente) e na Estratégia de Dados da ONU (ver glossário). Os documentos da União Europeia, como o Data Act (ver capítulo VIII) e o Data Governance Act (ver parágrafo 54), fundamentam as definições de interoperabilidade (também inspirada na Minuta supracitada) e espaço de dados (que renomeamos como “ecossistema de dados” conforme termo já utilizado no âmbito do SUS - ver art.3º), enquanto as Recomendações sobre Acesso e Compartilhamento de Dados da OCDE (ver item II) inspiram a definição de “ciclo de vida de dados”. Transversalmente, essas definições foram complementadas pelas disposições sobre dados no Pacto Global Digital da ONU (ver parágrafos 37, 41, 48), e no Plano Brasileiro de Inteligência Artificial (PBIA) (ver ação 28), especialmente no que tange a interoperabilidade e governança

de dados. Além disso, as definições baseiam-se em documentos que enfatizam perspectivas do Sul Global e aspectos de justiça de dados e soberania digital, como a Data Policy Framework da União Africana (ver capítulo 5), a Declaração de São Luís de grupos de engajamento do G20 (ver parágrafo 3) e a Declaração de Líderes dos BRICS sobre governança global da Inteligência Artificial (ver Parágrafo “A Soberania Digital e o Direito ao Desenvolvimento são Fundamentais para a Governança Global da IA”).

REDAÇÃO ATUAL

Art. 3º O desenvolvimento, a implementação e o uso de sistemas de IA observarão a boa-fé e os seguintes princípios:

XV – promoção da interoperabilidade de sistemas de IA para permitir acesso mais amplo e inovação colaborativa

PROPOSTA

Art. 3º O desenvolvimento, a implementação e o uso de sistemas de IA observarão a boa-fé e os seguintes princípios:

XV – promoção da interoperabilidade de sistemas de IA e de dados para permitir acesso mais amplo, inovação colaborativa e livre iniciativa;

XIX - soberania e autonomia tecnológica para o desenvolvimento cultural, socioeconômico e bem-estar da população brasileira

REDAÇÃO ATUAL

Art. 4º Para os fins desta Lei, adotam-se as seguintes definições:

I – sistema de inteligência artificial (IA): (...)

XXX – risco sistêmico: potenciais efeitos adversos negativos decorrentes de um sistema de IA de propósito geral e generativa com impacto significativo sobre direitos fundamentais individuais e sociais.

PROPOSTA

Art. 4º Para os fins desta Lei, adotam-se as seguintes definições:

I – sistema de inteligência artificial (IA): (...)

XXX – risco sistêmico: potenciais efeitos adversos negativos decorrentes de um sistema de IA

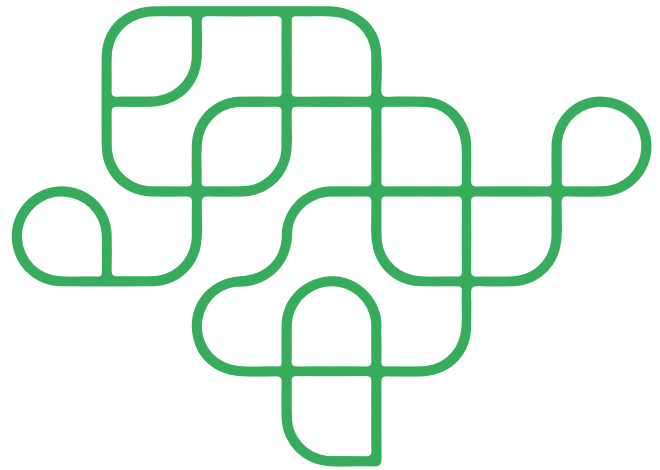
de propósito geral e generativa com impacto significativo sobre direitos fundamentais individuais e sociais.

XXX - interoperabilidade de dados: a capacidade de diferentes sistemas, organizações e setores compartilharem, acessarem, utilizarem e reutilizarem dados de forma segura, ética, eficiente e condizente com direitos fundamentais e demais legislações em vigor, inclusive por meio de ecossistemas de dados, na forma da lei.

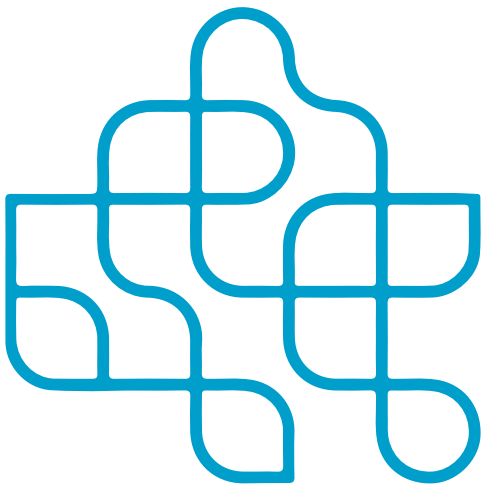
XXX - ecossistemas de dados: infraestruturas que viabilizam o compartilhamento estruturado e responsável de dados entre entes públicos, privados e da sociedade civil, com vistas à inovação, à transparência, à geração de valor, à eficiência de políticas públicas e ao desenvolvimento social e econômico de soluções baseadas em inteligência artificial.

XXX - ciclo de vida de dados: abrange todas as operações realizadas sobre os dados, sejam automatizadas ou manuais, desde sua origem até seu eventual descarte, envolvendo a criação, coleta, organização, validação, armazenamento, processamento, análise, disseminação, uso, compartilhamento, arquivamento e exclusão de dados.

XXX - governança de dados: conjunto de estruturas, normas, estratégias e mecanismos de diálogo que regulam o uso de dados de forma legal, ética, segura e acessível, visando à conformidade regulatória e à promoção do desenvolvimento socioeconômico justo à nível local e global.



02. DOS DIREITOS FUNDAMENTAIS



02. DOS DIREITOS FUNDAMENTAIS

Direito de oposição ao tratamento automatizado de dados pessoais para usos em sistemas de IA

JUSTIFICATIVA

Um dos gargalos do regime jurídico de proteção de dados pessoais no Brasil hoje é a baixa efetividade dos direitos de oposição, garantidos no artigo 18, §2º, da Lei 13.709/2018.

Tal problema tem se agravado a partir da tomada de decisão de diversas grandes empresas de tecnologia (por exemplo: X, LinkedIn, Meta) de utilizar automaticamente os dados pessoais de seus usuários para treinamento de sistemas de IA.

O que deveria ser um direito fundamental básico, que seria se opor ao tratamento de dados pessoais que pretende ser utilizado para uma nova finalidade, passou a ser uma barreira e um obstáculo intransponível. Sob a justificativa de tratamento dos dados com base no legítimo interesse (uma das hipóteses legais de tratamento de dados previsto na LGPD), as empresas passaram a descartar a autonomia do usuário, iniciando processos definidos por padrão, mediante atualização de seus Termos de Uso e Políticas de Privacidade, para tratamento de dados pessoais para treinamento de sistemas de aprendizado por máquinas.

A ANPD já se posicionou contundentemente em seu Guia sobre o Legítimo Interesse que a garantia do direito de oposição é essencial para a autodeterminação informativa e a concretização do princípio da boa fé no tratamento de dados. Entretanto, a atuação da ANPD e os mecanismos existentes têm se mostrado insuficiente para lidar com a atuação coordenada de várias empresas que desenvolvem sistemas de IA. É preciso que exista o reconhecimento de um direito fundamental à oposição do tratamento de dados pessoais para treinamento de sistemas de inteligência artificial, sendo esta uma manifestação da autonomia e dignidade da pessoa humana.

REDAÇÃO ATUAL

Art. 5º A pessoa ou grupo afetado por sistema de IA, independentemente do seu grau de risco, tem os seguintes direitos, a serem exercidos na forma e nas condições descritas neste Capítulo:

I – direito à informação quanto às suas interações com sistemas de IA, de forma acessível, gratuita e de fácil compreensão, inclusive sobre caráter automatizado da interação, exceto nos casos em que se trate de sistemas de IA dedicados única e exclusivamente à cibersegurança e à ciberdefesa, conforme regulamento;

II – direito à privacidade e à proteção de dados pessoais, em especial os direitos dos titulares de dados nos termos da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), e da legislação pertinente;

III – direito à não discriminação ilícita ou abusiva e à correção de vieses discriminatórios ilegais ou abusivos, sejam eles diretos ou indiretos.

§ 1º A informação referida no inciso I do caput deste artigo será fornecida com o uso de ícones ou símbolos uniformizados facilmente reconhecíveis, sem prejuízo de outros formatos.

§ 2º 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.

PROPOSTA

Art. 5º A pessoa ou grupo afetado por sistema de IA, independentemente do seu grau de risco, tem os seguintes direitos, a serem exercidos na forma e nas condições descritas neste Capítulo:

I – direito à informação quanto às suas interações com sistemas de IA, de forma acessível, gratuita e de fácil compreensão, inclusive sobre caráter automatizado da interação, exceto nos casos em que se trate de sistemas de IA dedicados única e exclusivamente à cibersegurança e à ciberdefesa, conforme regulamento;

II – direito à privacidade e à proteção de dados pessoais, em especial os direitos dos titulares de dados nos termos da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), e da legislação pertinente;

III – direito à não discriminação ilícita ou abusiva e à correção de vieses discriminatórios ilegais ou abusivos, sejam eles diretos ou indiretos.

IV - direito à oposição ao tratamento de dados pessoais para composição de bases de dados e treinamento de sistemas de inteligência artificial;

§ 1º A informação referida no inciso I do caput deste artigo será fornecida com o uso de ícones ou símbolos uniformizados facilmente reconhecíveis, sem prejuízo de outros formatos.

§ 2º 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.

Desinformação (direito à informação clara, mecanismos de integridade, letramento digital)

JUSTIFICATIVA

A capacidade dos sistemas de Inteligência Artificial de gerar conteúdos sintéticos (textos, imagens, vídeos e áudios falsos) impõe sérios riscos à integridade da informação e à confiança nas instituições democráticas, na ciência e nas relações de consumo. Tais riscos afetam tanto a esfera coletiva, por meio da manipulação da opinião pública, quanto a esfera individual, ao induzir comportamentos prejudiciais à saúde, segurança ou autonomia dos indivíduos.

Apesar de o PL 2338/2023 reconhecer a importância da informação íntegra e segura, conforme dispostos nos fundamentos do art. 2º e no art. 5º (direito à informação adequada e clara), a proposta normativa ainda carece de instrumentos específicos para enfrentamento à desinformação gerada por IA, especialmente no que se refere a:

- Sinalização obrigatória de conteúdos modificados por IA;
- Mecanismos de integridade e auditoria voltados para combate à desinformação;
- Políticas públicas de letramento digital com foco em pensamento crítico e identificação de conteúdos manipulados.

Embora o Brasil ainda não disponha de uma legislação específica voltada aos crimes de desinformação, o ordenamento jurídico vigente já contempla dispositivos relevantes que podem ser aplicados a esse fenômeno. Um exemplo importante é o Código de Defesa do Consumidor, cujos artigos 66 a 69 tipificam penalmente práticas publicitárias enganosas ou omissivas, inclusive quando essas práticas são potencializadas por tecnologias como a inteligência artificial.

Países como Itália aprovaram legislações com normas específicas para conter o uso ilícito de IA em processos de desinformação e danos democráticos (ver legislação aprovada no Senado da Itália).

Nesse contexto, é fundamental que o Projeto de Lei 2338/2023, que trata da regulação da IA no Brasil, seja desenvolvido em harmonia com os marcos legais já existentes, assegurando coerência normativa e evitando sobreposições ou lacunas regulatórias.

Mais do que isso, é necessário que o PL promova a responsabilização efetiva dos agentes envolvidos na produção e disseminação de conteúdos desinformativos, especialmente quando houver intenção manipulativa ou risco concreto à ordem pública, à saúde ou à integridade de grupos vulneráveis.

REDAÇÃO ATUAL

Art. 5º A pessoa ou grupo afetado por sistema de IA, independentemente do seu grau de risco, tem os seguintes direitos, a serem exercidos na forma e nas condições descritas neste Capítulo:

I – direito à informação quanto às suas interações com sistemas de IA, de forma acessível, gratuita e de fácil compreensão, inclusive sobre caráter automatizado da interação, exceto nos casos em que se trate de sistemas de IA dedicados única e exclusivamente à cibersegurança e à ciberdefesa, conforme regulamento;

II – direito à privacidade e à proteção de dados pessoais, em especial os direitos dos titulares de dados nos termos da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), e da legislação pertinente;

III – direito à não discriminação ilícita ou abusiva e à correção de vieses discriminatórios ilegais ou abusivos, sejam eles diretos ou indiretos.

§ 1º A informação referida no inciso I do caput deste artigo será fornecida com o uso de ícones ou símbolos uniformizados facilmente reconhecíveis, sem prejuízo de outros formatos.

§ 2º 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.

PROPOSTA

Art. 5º A pessoa ou grupo afetado por sistema de IA, independentemente do seu grau de risco, tem os seguintes direitos, a serem exercidos na forma e nas condições descritas neste Capítulo:

I – direito à informação quanto às suas interações com sistemas de IA, de forma acessível, gratuita e de fácil compreensão, inclusive sobre caráter automatizado da interação, exceto nos casos em que se trate de sistemas de IA dedicados única e exclusivamente à cibersegurança e à ciberdefesa, conforme regulamento;

II – direito à privacidade e à proteção de dados pessoais, em especial os direitos dos titulares de dados nos termos da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), e da legislação pertinente;

III – direito à não discriminação ilícita ou abusiva e à correção de vieses discriminatórios ilegais ou abusivos, sejam eles diretos ou indiretos.

IV - direito à oposição ao tratamento de dados pessoais para composição de bases de dados e treinamento de sistemas de inteligência artificial;

§ 3º Sempre que a informação veiculada por sistemas de IA tiver finalidade comercial ou publicitária, deverá ser expressamente sinalizado se o conteúdo foi gerado ou modificado por sistemas automatizados, inclusive com a indicação de que se trata de conteúdo sintético.

REDAÇÃO ATUAL

Art. 40 Os agentes de IA poderão, individualmente ou por meio de associações, formular códigos de boas práticas e de governança que estabeleçam:

(...)

VII – disponha de mecanismos e procedimentos internos de integridade, de auditoria, de incentivo à denúncia de irregularidades e de aplicação efetiva de códigos de ética.

PROPOSTA

Art. 40 Os agentes de IA poderão, individualmente ou por meio de associações, formular códigos de boas práticas e de governança que estabeleçam:

(...)

VII – disponha de mecanismos e procedimentos internos de integridade, de auditoria, **com foco no combate à desinformação**, de incentivo à denúncia de irregularidades e de aplicação efetiva de códigos de ética;

REDAÇÃO ATUAL

Art. 70 A administração pública, no âmbito da União, dos Estados, do Distrito Federal e dos Municípios, implementará programas de:

II – letramento digital para uso significativo, responsável e com equidade dos sistemas de IA disponíveis, priorizando-se a educação básica.

PROPOSTA

Art. 70 A administração pública, no âmbito da União, dos Estados, do Distrito Federal e dos Municípios, implementará programas de:

II – letramento digital para uso significativo, responsável, crítico e com equidade dos sistemas de IA disponíveis, priorizando-se a educação básica, com base em diretrizes nacionais de alfabetização midiática, **sob a orientação do programa Mais Ciência**.

Direito à não manipulação enganosa

JUSTIFICATIVA

Os estudos de psicologia e medicina produzidos nos últimos anos apontam três tipos de danos às pessoas com relação aos usos de IA. O primeiro é chamado de “efeito bajulador”, que é um viés de confirmação permanente sobre as opiniões humanas, considerando que os sistemas são programados para agradar o usuário e engajar mediante linguagem natural.

O segundo dano é a antropomorfização dos sistemas de IA, em especial os modelos de linguagem natural, que simulam a relação social com uma pessoa humana, produzindo uma sensação de estar em relação com uma pessoa e não um sistema de IA. Esse fenômeno é bem documentado em estudos de HCI (Human-Computer Interaction), psicologia social e ciências cognitivas. Isso está associado a mecanismos cognitivos de teoria da mente e a heurísticas sociais automáticas. A antropomorfização pode ser especialmente nociva para o desenvolvimento cerebral de crianças e adolescentes, que ainda não possuem o desenvolvimento pleno do córtex frontal e de outras regiões do cérebro responsáveis pelo julgamento moral e processos de tomada de decisão (que se desenvolvem até os 25 anos). A antropomorfização é reconhecida como um problema para autonomia e bem-estar por pesquisadores do Google Deep Mind.

O terceiro dano é o risco de que o uso excessivo de sistemas de IA leve alguns indivíduos a estados de paranoia ou distorção da realidade. Esse risco é particularmente relevante para pessoas com condições de saúde mental como transtorno bipolar, borderline ou outros quadros que já afetam a estabilidade da percepção da realidade. Nessas situações, a interação intensa com IA pode agravar vulnerabilidades psicológicas, aumentando a suscetibilidade à manipulação e contribuindo para consequências sérias, como isolamento social e risco de autolesão. Trata-se de uma preocupação legítima em saúde mental.

Um antídoto a esses danos é o reconhecimento de um direito fundamental à não manipulação por sistemas de Inteligência Artificial, tal como reconhecido em legislações contemporâneas (o artigo 5º do AI Act impede técnicas de manipulação habilitadas por IA, que podem ser usadas para persuadir as pessoas a se envolverem em comportamentos indesejados ou para enganá-las, induzindo-as a tomar decisões de uma forma que subverta e prejudique sua autonomia). Propomos, assim, que exista o direito fundamental à não manipulação por sistemas de inteligência artificial de forma prejudicial à autonomia humana.

A consequência prática do reconhecimento de um direito fundamental à não manipulação é a mudança de condutas e práticas dos desenvolvedores, que passam a assumir um ônus de construir designs que limitem a antropomorfização de sistemas interativos.

REDAÇÃO ATUAL

Art. 5º A pessoa ou grupo afetado por sistema de IA, independentemente do seu grau de risco, tem os seguintes direitos, a serem exercidos na forma e nas condições descritas neste Capítulo:

I – direito à informação quanto às suas interações com sistemas de IA, de forma acessível, gratuita e de fácil compreensão, inclusive sobre caráter automatizado da interação, exceto nos casos em que se trate de sistemas de IA dedicados única e exclusivamente à cibersegurança e à ciberdefesa, conforme regulamento;

II – direito à privacidade e à proteção de dados pessoais, em especial os direitos dos titulares de dados nos termos da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), e da legislação pertinente;

III – direito à não discriminação ilícita ou abusiva e à correção de vieses discriminatórios ilegais ou abusivos, sejam eles diretos ou indiretos.

§ 1º A informação referida no inciso I do caput deste artigo será fornecida com o uso de ícones ou símbolos uniformizados facilmente reconhecíveis, sem prejuízo de outros formatos.

§ 2º 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.

PROPOSTA

Art. 5º A pessoa ou grupo afetado por sistema de IA, independentemente do seu grau de risco, tem os seguintes direitos, a serem exercidos na forma e nas condições descritas neste Capítulo:

I – direito à informação quanto às suas interações com sistemas de IA, de forma acessível, gratuita e de fácil compreensão, inclusive sobre caráter automatizado da interação, exceto nos casos em que se trate de sistemas de IA dedicados única e exclusivamente à cibersegurança e à ciberdefesa, conforme regulamento;

II – direito à privacidade e à proteção de dados pessoais, em especial os direitos dos titulares de dados nos termos da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), e da legislação pertinente;

III – direito à não discriminação ilícita ou abusiva e à correção de vieses discriminatórios ilegais ou abusivos, sejam eles diretos ou indiretos.

IV - direito à oposição ao tratamento de dados pessoais para composição de bases de dados e treinamento de sistemas de inteligência artificial;

V - direito à não manipulação abusiva por sistemas de inteligência artificial de forma prejudicial à autonomia da pessoa humana;

§ 1º A informação referida no inciso I do caput deste artigo será fornecida com o uso de ícones ou símbolos uniformizados facilmente reconhecíveis, sem prejuízo de outros formatos.

§ 2º 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 consider

Direitos de participação em avaliações de impacto algorítmicos

JUSTIFICATIVA

Em sistemas de IA de alto risco, a legislação determina o direito à explicação, o direito à contestação, o direito de solicitação de revisão de decisões e o direito de revisão humana de decisões.

Uma lacuna importante do regramento do art. 6º é a definição de direitos de participação, que devem ser exercidos como um mecanismo de fortalecimento da vida cívica e da democracia. Esse ponto é defendido claramente por Margot Kaminski e Gianclaudio Malgieri no importante estudo “Impacted Stakeholder Participation in AI and Data Governance”, publicado pela Universidade de Yale em 2025. Nesse texto, eles argumentam que as partes interessadas afetadas por sistemas de IA devem ser vistas como titulares de direitos (“impacted rights-holders”) que possuem novos direitos substanciais de participação.

Tendo em mente os valores da legislação de centralidade da pessoa humana, livre desenvolvimento da personalidade, promoção do pleno desenvolvimento e do exercício da cidadania e proteção e promoção de direitos de grupos vulneráveis (fundamentos do art. 2º), propomos o reconhecimento explícito de direitos de participação de grupos vulneráveis em procedimentos de avaliação de impacto a direitos fundamentais em sistemas de alto risco.

A previsão do direito de participação em avaliações preliminares e avaliações de impactos algorítmicos busca assegurar que os sistemas de inteligência artificial de alto risco sejam objeto de processos transparentes e inclusivos, de modo a considerar não apenas os interesses econômicos e tecnológicos, mas também os direitos fundamentais das pessoas potencialmente afetadas.

O §3º reforça esse compromisso democrático ao permitir que o direito de participação seja exercido coletivamente por organizações civis, ampliando a efetividade desse mecanismo. Essa solução evita a dispersão de vozes individuais, fortalece a representação de interesses coletivos e difusos e garante que comunidades afetadas tenham espaço legítimo de manifestação. Trata-se de instrumento alinhado às melhores práticas de governança participativa e de proteção de direitos em contextos regulatórios complexos.

O §4º complementa essa lógica ao estabelecer que a avaliação de impacto em sistemas de IA de alto risco deve identificar riscos específicos para grupos vulneráveis. Essa exigência é crucial porque tais grupos — como crianças, adolescentes, idosos, pessoas com deficiência ou populações em situação de vulnerabilidade social — estão mais sujeitos a sofrer danos desproporcionais decorrentes de vieses ou falhas tecnológicas. Convocá-los a participar do processo decisório é medida que concretiza os princípios da igualdade material, da não discriminação e da dignidade da pessoa humana, pilares da Constituição Federal.

REDAÇÃO ATUAL

Art. 6º A pessoa ou grupo afetado por sistema de IA de alto risco tem os seguintes direitos:

I – direito à explicação sobre a decisão, a recomendação ou a previsão feitas pelo sistema;

II – direito de contestar e de solicitar a revisão de decisões, recomendações ou previsões de sistema de IA;

III – direito à revisão humana das decisões, levando-se em conta o contexto, o risco e o estado da arte do desenvolvimento tecnológico.

§ 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.

§ 2º Os direitos previstos nesta Seção serão implementados considerando o estado da arte do desenvolvimento tecnológico, devendo o agente do sistema de IA de alto risco sempre implementar medidas eficazes e proporcionais.

PROPOSTA

Art. 6º A pessoa ou grupo afetado por sistema de IA de alto risco tem os seguintes direitos:

I – direito à explicação sobre a decisão, a recomendação ou a previsão feitas pelo sistema;

II – direito de contestar e de solicitar a revisão de decisões, recomendações ou previsões de sistema de IA;

III – direito à revisão humana das decisões, levando-se em conta o contexto, o risco e o estado da arte do desenvolvimento tecnológico.

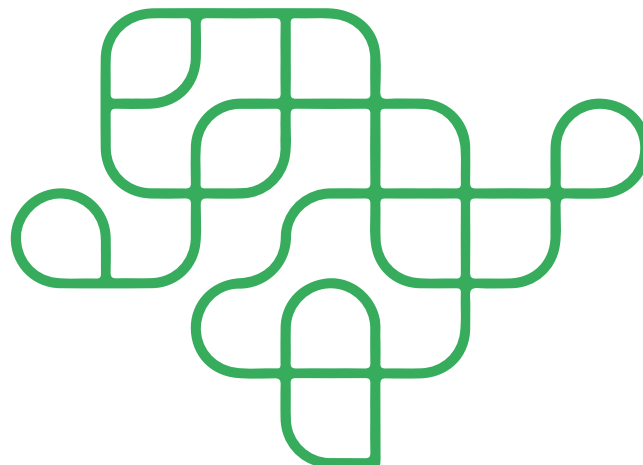
IV - direito de participação em avaliações preliminares e avaliações de impactos algorítmicos, que devem considerar seus interesses e eventuais oposições a sistemas e aplicações na avaliação dos riscos e implementação de medidas de mitigação;

§ 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.

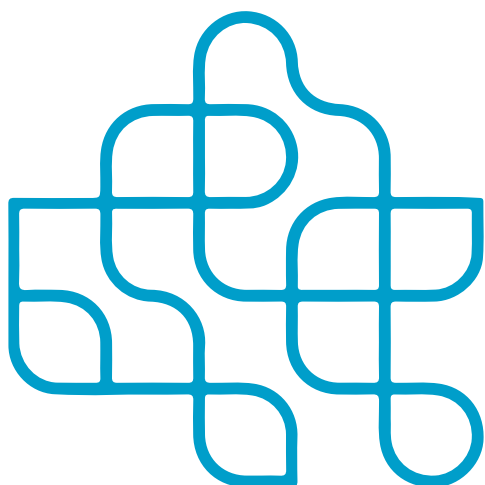
§ 2º Os direitos previstos nesta Seção serão implementados considerando o estado da arte do desenvolvimento tecnológico, devendo o agente do sistema de IA de alto risco sempre implementar medidas eficazes e proporcionais.

§3º O direito de participação referido no inciso IV poderá ser exercido coletivamente mediante representação por organizações civis que representam interesses coletivos e difusos;

§4º A avaliação de impacto em sistemas de IA de alto risco deve incluir a identificação de riscos específicos de danos que possam ter impacto nos direitos fundamentais de pessoas ou grupos vulneráveis, devendo tais grupos serem convocados a exercer seus direitos de participação.



03. CLASSIFICAÇÃO E CATEGORIAS DE RISCO



03. CLASSIFICAÇÃO E CATEGORIAS DE RISCO

Do Alto Risco

JUSTIFICATIVA

O Pacto Global Digital da ONU (2024) já reconheceu que uma governança de dados responsável e interoperável (ver parágrafo 37) é essencial para a proteção dos direitos humanos, promoção de crescimento econômico e desenvolvimento, além de promoção da inovação. Assim, os princípios se baseiam em padrões já estabelecidos nacional e internacionalmente, assegurando que uma coleta de dados e todo seu ciclo de vida sejam proporcionais, seguros, com fins legítimos. Além disso, princípios como sustentabilidade, igualdade de gênero, inclusão significativa, acesso, e cooperação internacional, também já estão consensuadas pelo Pacto, do qual o Brasil é signatário (ver parágrafo 8).

Em termos regulatórios, a União Europeia apresenta o precedente do Data Governance Act, visto como um instrumento regulatório para uso e reuso de dados entre diferentes setores, incluindo o setor público (ver item “Reuse of certain categories of data held by public sector bodies”). O AI Act da UE, similarmente, baseia-se numa classificação de riscos para os sistemas de IA (ver capítulo III), definindo diretrizes específicas sobre governança de dados para sistemas de alto risco.

REDAÇÃO ATUAL

Art. 16. A regulamentação da lista e a classificação de novas aplicações de sistemas de IA de alto risco serão precedidas de procedimento que garanta participação social e de análise de impacto regulatório, cabendo:

II – às autoridades setoriais, no âmbito de suas atribuições e em caráter prevalente, dispor sobre os aspectos técnicos e específicos de aplicações de IA no mercado regulado, devendo:

a) estabelecer listas sobre hipóteses classificadas ou não classificadas como de alto risco dentro das finalidades e contextos definidos no art. 14;

b) estabelecer, com precisão, o rol de sistemas de alto risco desta Lei;

c) receber e analisar as avaliações de impacto algorítmico;

d) indicar, em lista, casos de utilização de sistemas ou aplicações de sistemas de IA de alto risco ou não.

PROPOSTA

Art. 16. A regulamentação da lista e a classificação de novas aplicações de sistemas de IA de alto risco serão precedidas de procedimento que garanta participação social e de análise de impacto regulatório, cabendo:

II – às autoridades setoriais, no âmbito de suas atribuições e em caráter prevalente, dispor sobre os aspectos técnicos e específicos de aplicações de IA no mercado regulado, devendo:

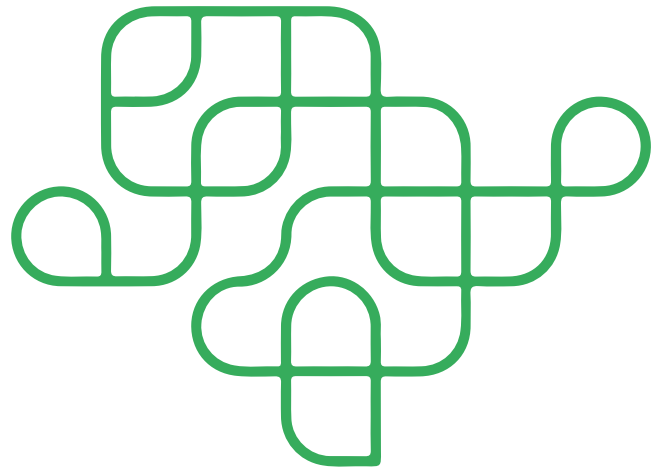
a) estabelecer listas sobre hipóteses classificadas ou não classificadas como de alto risco dentro das finalidades e contextos definidos no art. 14;

b) estabelecer, com precisão, o rol de sistemas de alto risco desta Lei;

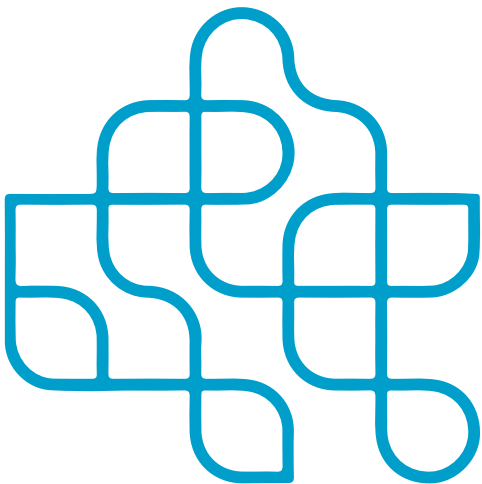
c) receber e analisar as avaliações de impacto algorítmico;

d) indicar, em lista, casos de utilização de sistemas ou aplicações de sistemas de IA de alto risco ou não;

e) disponibilizar mecanismos de correção e mitigação de dados enviesados, incorretos, e que possam causar discriminação.



04. AVALIAÇÕES DE IMPACTO ALGORÍTMICO



04. AVALIAÇÕES DE IMPACTO ALGORÍTMICO

Procedimentalização de avaliações de impacto algorítmico e supressão de poderes normativos de autoridades setoriais sobre a procedimentalização da AIA

JUSTIFICATIVA

A avaliação de impacto algorítmico é um instrumento central da legislação de Inteligência Artificial. No entanto, a primeira versão do projeto de lei não previa uma metodologia adequada para a elaboração da AIA. Ela ficou delegada a regulamentação de autoridades setoriais, bem como de casos de flexibilização mesmo em sistemas de alto risco.

O problema disso é o atraso na fiscalização adequada da lei. Isto pois o AIA é um instrumento pelo qual as autoridades podem avaliar se o agente regulado cumpriu com suas obrigações perante à lei. Se for preciso que cada setor aguarde cada autoridade setorial regulamentar para que se possa cobrar efetivamente o cumprimento da lei, é possível que também atrasemos uma fiscalização adequada e justa.

Uma avaliação de impacto algorítmica com processos bem definidos e detalhados são facilitadores da conformidade com a Lei. Isto pois tais avaliações permitem com que o SIA avalie de fato quais disposições são aplicáveis e o que cada empresa precisa fazer

Essa situação também cria uma quebra de isonomia entre os agentes regulados: se algumas autoridades setoriais puderem regulamentar o instrumento antes das demais, aquelas que se atrasarem na regulação acabarão aplicando as regras em um momento posterior, revelando uma mudança de tratamento entre os agentes regulados.

Sem uma metodologia mínima, existe um risco de que fornecedores de IA produzam avaliações de impacto regulatório de forma inconsistente, abrindo espaço para baixa atividade da norma e violações à lei e direitos fundamentais, ainda que tais fornecedores ajam de boa-fé. Nesse cenário, tais regulados podem até ser sancionados por não adotarem uma metodologia adequada do instrumento. Adicionar uma metodologia mínima reduziria drasticamente esse risco.

REDAÇÃO ATUAL

Inexistente

PROPOSTA

Art. 25-B. A metodologia da avaliação de impacto conterá, ao menos, as seguintes etapas:

- I – preparação;
- II – cognição do risco;
- III – mitigação dos riscos encontrados;
- IV – monitoramento.

§ 1º A avaliação de impacto considerará e registrará, ao menos:

- a) riscos conhecidos e previsíveis associados ao sistema de inteligência artificial à época em que foi desenvolvido, bem como os riscos que podem razoavelmente dele se esperar;
- b) benefícios associados ao sistema de inteligência artificial;
- c) probabilidade de consequências adversas, incluindo o número de pessoas potencialmente impactadas e o esforço necessário para mitigá-las;
- e) lógica de funcionamento do sistema de inteligência artificial;
- f) processo e resultado de testes e avaliações e medidas de mitigação realizadas para verificação de possíveis impactos a direitos, com especial destaque para potenciais impactos discriminatórios;
- g) treinamento e ações de conscientização dos riscos associados ao sistema de inteligência artificial;
- h) medidas de mitigação e indicação e justificação do risco residual do sistema de inteligência artificial, acompanhado de testes de controle de qualidade frequentes; e
- i) medidas de transparência ao público, especialmente aos potenciais usuários do sistema, a respeito dos riscos residuais, principalmente quando envolver alto grau de nocividade ou periculosidade à saúde ou segurança dos usuários, nos termos dos artigos 9º e 10 da Lei nº 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor).

Art. 25-C. A avaliação de impacto de sistemas de inteligência artificial seguirá procedimento simplificado, composto, no mínimo, pelas seguintes etapas:

- I – preparação, com a definição do escopo, objetivos e responsáveis pela avaliação;
- II – identificação e análise de riscos, compreendendo os perigos conhecidos, previsíveis e razoáveis, considerando o estágio de desenvolvimento do sistema;
- III – avaliação dos efeitos potenciais, abrangendo benefícios esperados, lógica de funcionamento do sistema de inteligência artificial, probabilidade de consequências adversas e número de pessoas potencialmente impactadas;
- IV – mitigação, com a descrição das medidas adotadas, justificação dos riscos residuais e mecanismos de controle e monitoramento contínuo.

JUSTIFICATIVA

Foram propostas mudanças para harmonizar o desenho do SIA e evitar inconsistências normativas. Na redação atual, o texto tem uma ambiguidade que dá a entender que as autoridades setoriais podem definir critérios, período de atuação e flexibilizações do instrumento. Essa situação poderia levar a uma ocasião em que uma autoridade setorial regulamente o AIA e depois precise adaptar as suas disposições ao regulamento geral sobre o tema emitido pela autoridade competente.

Além de criar uma grave insegurança jurídica, a redação atual do art 25 contraria as competências da autoridade competente em harmonizar a regulação de inteligência artificial, dispostas no art. 46, II, b .

Também foi incluído um trecho de que o AIA deve ser feito a partir de participação pública, conferindo a possibilidade de flexibilização dada pelo próprio SIA. A necessidade de participação pública se justifica em razão de se tratarem de sistemas de alto risco. Contudo, ela não é absoluta e pode ser flexibilizada ou até derogada pela análise do SIA, garantindo equilíbrio entre o requisito e casos em que ele não será necessário.

REDAÇÃO ATUAL

Art. 25. A avaliação de impacto algorítmico de sistemas de IA é obrigação do desenvolvedor ou do aplicador que introduzir ou colocar sistema de IA em circulação no mercado, sempre que o sistema ou o seu uso forem de alto risco, considerando o papel e a participação do agente na cadeia.

§ 1º O desenvolvedor de sistema de IA de alto risco deverá, nos termos de regulamento, compartilhar com a autoridade setorial as avaliações preliminares e de impacto algorítmico, cuja metodologia considerará e registrará, ao menos, avaliação dos riscos e benefícios aos direitos fundamentais, medidas de atenuação e efetividade dessas medidas de gerenciamento.

§ 2º O agente de IA poderá requerer junto aos demais agentes da cadeia, respeitados os segredos industriais e comerciais, as informações necessárias para a realização da avaliação de impacto algorítmico.

§ 3º A avaliação deverá ser realizada em momento prévio e de acordo com o contexto específico da introdução ou colocação em circulação no mercado do sistema de IA.

§ 4º Caberá à autoridade setorial definir as hipóteses em que a avaliação de impacto algorítmico será flexibilizada, levando em consideração o contexto de atuação e o papel de cada um dos agentes de IA e as normas gerais da autoridade competente.

§ 5º A autoridade competente, a partir das diretrizes do Cria, estabelecerá critérios gerais e elementos para a elaboração de avaliação de impacto algorítmico e a periodicidade de sua atualização, considerando o ciclo de vida dos sistemas de IA de alto risco.

§ 6º Caberá à autoridade setorial, a partir do estado da arte do desenvolvimento tecnológico e das melhores práticas, a regulamentação dos critérios e da periodicidade de atualização das avaliações de impacto algorítmico, considerando o ciclo de vida dos sistemas de IA de alto risco.

§ 7º Os agentes de IA que, posteriormente à introdução de sistema de IA no mercado ou à sua utilização em serviço, tiverem conhecimento de risco ou impacto inesperado e relevante que o sistema apresente a direitos de pessoas naturais comunicarão o fato imediatamente à autoridade setorial e aos outros agentes na cadeia para que sejam tomadas todas as medidas cabíveis, inclusive, quando necessário, a de notificar pessoas e grupos afetados pelo sistema de IA.

§ 8º Caberá à autoridade competente e às autoridades setoriais estabelecer as hipóteses em que a participação pública será necessária, assim como as hipóteses em que poderá ser realizada de maneira simplificada, indicando os critérios para essa participação.

PROPOSTA

Art. 25. A avaliação de impacto algorítmico de sistemas de IA é obrigação do desenvolvedor ou do aplicador que introduzir ou colocar sistema de IA em circulação no mercado, sempre que o sistema ou o seu uso forem de alto risco, considerando o papel e a participação do agente na cadeia.

§ 1º O desenvolvedor de sistema de IA de alto risco deverá, nos termos de regulamento, compartilhar com a autoridade setorial as avaliações preliminares e de impacto algorítmico, cuja metodologia considerará e registrará, ao menos, avaliação dos riscos e benefícios aos direitos fundamentais, medidas de atenuação e efetividade dessas medidas de gerenciamento.

§ 2º O agente de IA poderá requerer junto aos demais agentes da cadeia, respeitados os segredos industriais e comerciais, as informações necessárias para a realização da avaliação de impacto algorítmico.

§ 3º A avaliação deverá ser realizada em momento prévio e de acordo com o contexto específico da introdução ou colocação em circulação no mercado do sistema de IA.

~~§ 4º Caberá à autoridade setorial definir as hipóteses em que a avaliação de impacto algorítmico será flexibilizada, levando em consideração o contexto de atuação e o papel de cada um dos agentes de IA e as normas gerais da autoridade competente.~~

§ 4º A autoridade competente, a partir das diretrizes do Cria, estabelecerá **de forma prioritária** critérios gerais e elementos para a elaboração de avaliação de impacto algorítmico e a periodicidade de sua atualização, considerando o ciclo de vida dos sistemas de IA de alto risco. **As autoridades setoriais somente poderão regulamentar aspectos específicos após a publicação desse regulamento geral.**

~~§ 6º Caberá à autoridade setorial, a partir do estado da arte do desenvolvimento tecnológico e das melhores práticas, a regulamentação dos critérios e da periodicidade de atualização das avaliações de impacto algorítmico, considerando o ciclo de vida dos sistemas de IA de alto risco.~~

§ 5º Os agentes de IA que, posteriormente à introdução de sistema de IA no mercado ou à sua utilização em serviço, tiverem conhecimento de risco ou impacto inesperado e relevante que o sistema apresente a direitos de pessoas naturais comunicarão o fato imediatamente à autoridade setorial e aos outros agentes na cadeia para que sejam tomadas todas as medidas cabíveis, inclusive, quando necessário, a de notificar pessoas e grupos afetados pelo sistema de IA.

~~§ 8º Caberá à autoridade competente e às autoridades setoriais estabelecer as hipóteses em que a participação pública será necessária, assim como as hipóteses em que poderá ser reali-~~

~~zada de maneira simplificada, indicando os critérios para essa participação.~~

~~§ 6º A participação pública será obrigatória no processo de avaliação de impacto algorítmico. Somente após avaliação da autoridade competente, em cooperação com as autoridades setoriais, poderá haver simplificação ou dispensa dessa participação, com base em critérios previamente estabelecidos pela autoridade competente.~~

REDAÇÃO ATUAL

Art. 26. A avaliação de impacto algorítmico será realizada em momento anterior à introdução ou à colocação em circulação no mercado de sistema de IA, bem como consistirá em processo interativo contínuo, executado ao longo de todo o ciclo de vida dos sistemas de IA de alto risco, requeridas atualizações periódicas.

Parágrafo único. Considerando eventual regulamentação setorial existente, caberá à autoridade competente, em colaboração com as demais entidades do SIA, definir:

I – parâmetros gerais acerca da periodicidade de atualização das avaliações de impacto algorítmico, que devem ser realizadas ao menos quando da existência de alterações significativas nos sistemas, nos termos de regulamento;

II – as hipóteses em que a avaliação de impacto algorítmico será simplificada, considerando o tipo de agentes de sistemas de IA

PROPOSTA

Art. 26. A avaliação de impacto algorítmico será realizada em momento anterior à introdução ou à colocação em circulação no mercado de sistema de IA, bem como consistirá em processo interativo contínuo, executado ao longo de todo o ciclo de vida dos sistemas de IA de alto risco, requeridas atualizações periódicas.

Parágrafo único. **A autoridade competente, em colaboração com as demais entidades do SIA, deverá definir, de forma prioritária e anterior a qualquer regulamentação setorial sobre o tema:**

I – parâmetros gerais acerca da periodicidade de atualização das avaliações de impacto algorítmico, que devem ser realizadas ao menos quando da existência de alterações significativas nos sistemas, nos termos de regulamento;

II – critérios gerais a serem considerados na elaboração das avaliações de impacto algorítmico;

III – as hipóteses em que a avaliação de impacto algorítmico será simplificada, considerando o tipo de agentes de sistemas de IA.

JUSTIFICATIVA

Uma vez que a Avaliação de Impacto Algorítmico é exigida para sistemas de IA considerados como de alto risco, é preciso que os agentes façam a análise preliminar de seus sistemas antes de sua introdução no mercado.

Essa lógica é a parecida com a do Relatório de Impacto, onde a própria Autoridade nacional de proteção de dados recomenda “elaborar o RIPD antes de o controlador iniciar o tratamento dos dados pessoais para a finalidade desejada, justamente para que ele possa avaliar, de antemão, os possíveis riscos associados a esse tratamento.”¹

A obrigatoriedade da avaliação preliminar serve para a redução de encargos das empresas desenvolvedoras. Por um lado, permite com que elas tenham certeza da necessidade de se realizar um AIA. Por outro, a avaliação preliminar permite com que saibam de antemão o nível de risco de seus produtos e possam propor medidas de mitigação a partir do AIA. Nesse sentido, a avaliação preliminar é a porta de entrada para evitar danos ou perdas provocados por tais sistemas. Isso é relevante na medida em que tal análise permite identificar os usos esperados de uma IA, algo que pode salvaguardar organizações em caso de uso abusivo ou malicioso de tais tecnologias.

As mudanças propostas no seguinte artigo visam tornar o processo de avaliação preliminar algo de rotina de empresas do campo para avaliar se precisam ou não de uma avaliação de impacto algorítmica.

REDAÇÃO ATUAL

Art. 12. Antes de sua introdução e circulação no mercado, emprego ou utilização, o agente de IA poderá realizar avaliação preliminar para determinar o grau de risco do sistema, baseando-se nos critérios previstos neste Capítulo, de acordo com o estado da arte do desenvolvimento tecnológico.

§ 1º A realização da avaliação preliminar será considerada como medida de boa prática e poderá resultar em benefícios para o agente de IA para fins do disposto no art. 50, § 1º, podendo, inclusive, receber tratamento prioritário em procedimentos para avaliação de conformidade, nos termos do art. 34, ambos desta Lei.

§ 2º Caberá à autoridade setorial definir as hipóteses em que a avaliação preliminar será simplificada ou dispensada, observadas as normas gerais da autoridade competente.

§ 3º O agente poderá requerer junto aos demais agentes dos sistemas de IA informações que o capacitem a efetuar avaliação preliminar, nos termos desta Lei, respeitados os segredos comercial e industrial.

§ 4º Garantidos o contraditório e a ampla defesa, a autoridade competente poderá, em colaboração com as autoridades setoriais do SIA, determinar a reclassificação do sistema de IA,

¹ BRASIL. Autoridade Nacional de Proteção de Dados. Relatório de impacto à proteção de dados pessoais (RIPD). Brasília: ANPD, [2023?]

mediante notificação prévia, bem como determinar, de forma fundamentada, a realização de avaliação de impacto algorítmico.

§ 5º O resultado da avaliação preliminar poderá ser utilizado pelo agente de IA para demonstrar conformidade com os requisitos de segurança, transparência e ética previstos nesta Lei.

§ 6º A autoridade setorial poderá requerer a realização ou o acesso à avaliação preliminar do sistema de IA para fins de avaliação de risco do sistema, respeitados os segredos comercial e industrial.

PROPOSTA

Art. 12. Antes de sua introdução e circulação no mercado, emprego ou utilização, o agente de IA **deverá realizar avaliação preliminar** para determinar o grau de risco do sistema, baseando-se nos critérios previstos neste Capítulo, de acordo com o estado da arte do desenvolvimento tecnológico.

~~§ 1º A realização da avaliação preliminar será considerada como medida de boa prática e poderá resultar em benefícios para o agente de IA para fins do disposto no art. 50, § 1º, podendo, inclusive, receber tratamento prioritário em procedimentos para avaliação de conformidade, nos termos do art. 34, ambos desta Lei.~~

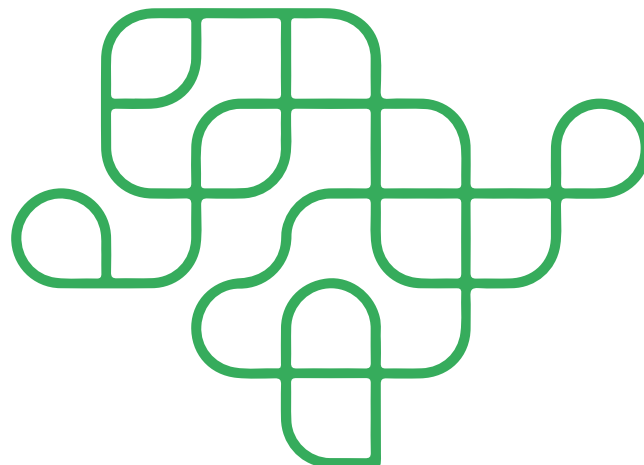
~~§ 1º Caberá à autoridade competente definir as hipóteses em que a avaliação preliminar poderá ser simplificada, observados critérios técnicos e o interesse público.~~

§ 2º O agente poderá requerer junto aos demais agentes dos sistemas de IA informações que o capacitem a efetuar a avaliação preliminar, nos termos desta Lei, respeitados os segredos comercial e industrial.

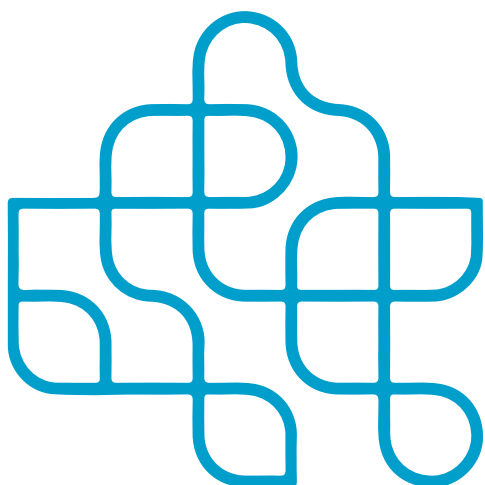
§ 3º Garantidos o contraditório e a ampla defesa, a autoridade competente poderá, em colaboração com as autoridades setoriais do SIA, determinar a reclassificação do sistema de IA, mediante notificação prévia, bem como determinar, de forma fundamentada, a realização de avaliação de impacto algorítmico.

§ 4º O resultado da avaliação preliminar poderá ser utilizado pelo agente de IA para demonstrar conformidade com os requisitos de segurança, transparência e ética previstos nesta Lei.

§ 5º A autoridade setorial poderá requerer a realização ou o acesso à avaliação preliminar do sistema de IA para fins de avaliação de risco do sistema, respeitados os segredos comercial e industrial.



05. BOAS PRÁTICAS E GOVERNANÇA



05. BOAS PRÁTICAS E GOVERNANÇA

Código de conduta e interoperabilidade de dados

JUSTIFICATIVA

A interoperabilidade de dados é um dos pilares de uma agenda de regulação que prevê menos concentração de mercado, menos barreiras à entrada e mais inovação em mercados digitais.

Seguindo a lógica estabelecida no art. 68 sobre as diretrizes para a atuação da União, dos Estados, do Distrito Federal e dos Municípios no desenvolvimento da IA no Brasil, e pela importância da interoperabilidade e uso dos dados para fins de políticas públicas, propõe-se o incentivo a essa mesma interoperabilidade para demais agentes de IA. Conforme a Minuta do Decreto que institui a Política de Governança de Dados, do Ministério da Gestão e Inovação em Serviços Públicos, futura legislação orientará os processos de interoperabilidade e compartilhamento de dados entre órgãos e entidades (ver capítulo II, V).

REDAÇÃO ATUAL

Art. 40. Os agentes de IA poderão, individualmente ou por meio de associações, formular códigos de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, inclusive sobre reclamações das pessoas afetadas, as normas de segurança, os padrões técnicos, as obrigações específicas para cada contexto setorial de implementação, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e as medidas de segurança técnicas e organizacionais apropriadas para a gestão dos riscos decorrentes da aplicação dos sistemas de IA no seu respectivo domínio de atividade.

...

§ 2º Os desenvolvedores e aplicadores de sistemas de IA, poderão implementar programa de governança que, de acordo com o estado da arte do desenvolvimento tecnológico:

...

Art. 41. Os agentes de IA podem associar-se voluntariamente sob a forma de pessoa jurídica de direito privado sem fins lucrativos para promover a autorregulação com o objetivo de incentivar e assegurar melhores práticas de governança ao longo de todo o ciclo de vida de sistemas de IA.

§ 1º A autorregulação pode compreender as seguintes funções:

PROPOSTA

Art. 40. Os agentes de IA poderão, individualmente ou por meio de associações, formular códigos de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, inclusive sobre reclamações das pessoas afetadas, as normas de segurança, os padrões técnicos, as obrigações específicas para cada contexto setorial de implementação, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e as medidas de segurança técnicas e organizacionais apropriadas para a gestão dos riscos decorrentes da aplicação dos sistemas de IA no seu respectivo domínio de atividade.

(...)

§ 2º Os desenvolvedores e aplicadores de sistemas de IA, poderão implementar programa de governança que, de acordo com o estado da arte do desenvolvimento tecnológico:

(...)

VIII - promova interoperabilidade entre os diferentes sistemas e entre dados, em especial com finalidade de interesse público, seguindo padrões, requisitos, e responsabilidades, observada a legislação aplicável.

JUSTIFICATIVA

A Ação 27 do PBIa sobre uma Nuvem Soberana está diretamente relacionada aos compromissos do Pacto Global Digital da ONU sobre “Bens Públicos Digitais” (parágrafos 14-17), e à Declaração de São Luís sobre Inteligência Artificial (2024) no âmbito do G20 (parágrafo 13). A ideia, que inclui dados e softwares abertos, é de empoderar as sociedades para que os dados sejam utilizados ao seu próprio benefício e desenvolvimento, facilitando investimentos e mecanismos de cooperação. Assim, a partir de uma infraestrutura pública digital e de uma governança de dados ética, o desenvolvimento de IAs soberanas estarão voltadas ao interesse público e desenvolvimento da própria população brasileira. Nesse mesmo sentido, o PBIa prevê o uso estratégico de dados nas Ações 28 e 29 do Eixo 3, sendo definidas medidas como o reuso e compartilhamento eficiente de dados, a fim de promover a interoperabilidade na administração pública e simplificar o acesso aos serviços públicos digitais. A Minuta da Política de Governança e Compartilhamento de Dados, similarmente, define diretrizes de interoperabilidade e compartilhamento de dados com a finalidade de atendimento do interesse público.

A relação entre governança de dados e inteligência artificial foi bastante debatida durante a presidência brasileira do G20, em 2024. A busca por uma abordagem de justiça de dados, e de integração entre os diferentes setores da sociedade, foi sintetizada na proposta do Think 20 (T20), grupo de engajamento de think tanks, e chamada de Data20 (D20).

Por fim, a inovação ética é uma abordagem já presente no Data Act da União Europeia, cujo incentivo para o uso colaborativo de dados também já foi analisado potencialmente no Brasil, pelo estudo realizado no Diálogo Digital Brasil-União Europeia. Esse tipo de inovação regulamentada aumenta a segurança jurídica, e também a confiança dos usuários sobre o compartilhamento de dados. A União Europeia também já aplica o uso de padrões internacionais para interoperabilidade, a exemplo do padrão ISO/IEC 19941:2017, por determinação do Data Act (parágrafo 90). O Data Policy Framework da União Africana, similarmente, reconhece a necessidade de promoção da interoperabilidade e compartilhamento, promovendo a abordagem de justiça de dados, através de iniciativas como o estabelecimento de padrões de dados abertos e o desenvolvimento de infraestruturas de dados regionais e continentais para promover o desenvolvimento da IA no continente.

REDAÇÃO ATUAL

Inexistente

PROPOSTA

Art. XX: A formulação, desenvolvimento e uso de sistemas de inteligência artificial pelo Poder Público devem observar práticas de governança de dados que promovam a interoperabilidade de abordagens nos níveis nacional, regional, e internacional, também com base em padrões abertos, e o compartilhamento e o reuso de dados de forma integrada, com finalidade de interesse público, equidade, proteção dos dados pessoais, e com promoção de inovação ética.

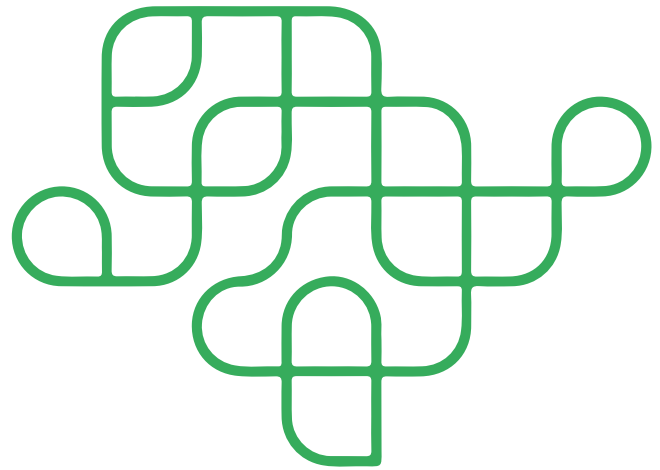
Parágrafo único. As práticas de governança de dados de promoção de interoperabilidade devem observar:

I - parâmetros técnicos de interoperabilidade consonantes com padrões já existentes, especialmente no âmbito internacional e órgãos de definição de padrões;

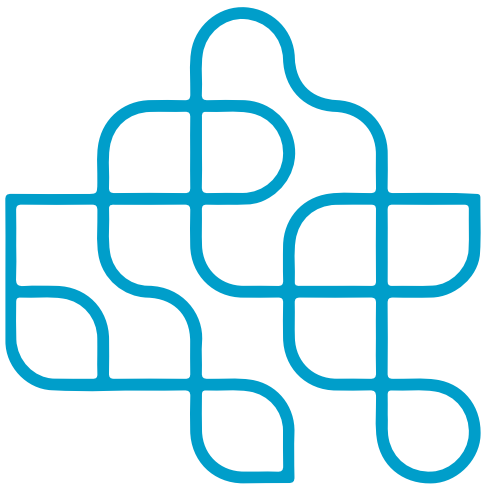
II - a padronização setorial em ecossistemas de dados específicos;

III - o envolvimento de agentes públicos e privados, incluindo a comunidade técnica e organizações da sociedade civil;

IV - a priorização de padrões que visem o interesse público.



06. SISTEMA NACIONAL DE REGULAÇÃO E GOVERNANÇA (SIA)



06. SISTEMA NACIONAL DE REGULAÇÃO E GOVERNANÇA (SIA)

ANPD, autoridades setoriais, aspectos concorrenciais, e multissetorialismo

JUSTIFICATIVA

O Pacto Global Digital da ONU (2024) em seu objetivo específico de governança de dados responsável e interoperável (ver Objetivo 4 e parágrafo 37) traz o compromisso de desenvolver padrões e trabalhar com auditorias regulares (ver item 42a).

Auditorias de avaliação de impacto são um componente regulatório central de normas contemporâneas de proteção de dados pessoais e de regulação de usos potencialmente abusivos de Inteligência Artificial.

Em linha com a estratégia brasileira de transformação digital e de compartilhamento de dados, incluímos entre as competências da autoridade setorial a instituição de ecossistemas de dados setoriais, permitindo que haja fomento à inovação e experimentação de usos estratégicos de dados em áreas como saúde e educação.

REDAÇÃO ATUAL

Art. 48. Compete à autoridade setorial:

- I – exercer competência regulatória, fiscalizatória e sancionatória, conforme sua esfera de competência outorgada por lei, para desenvolvimento, implementação e uso de sistemas de IA;
- II – expedir regras específicas para a aplicação de IA, incluindo aspectos relacionados a atividades de alto risco, observadas as normas gerais expedidas pela autoridade competente;
- III – promover e incentivar o disposto no Capítulo VI desta Lei para sistemas de IA que se inserem em sua esfera de competência outorgada por lei;
- IV – quanto à sua esfera de competência outorgada por lei, incentivar a adoção de padrões, melhores práticas e modelos de certificação e acreditação reconhecidos internacionalmente;
- V – supervisionar as medidas de governança adequadas a cada aplicação ou uso de sistemas de IA que classifique como de alto risco, de forma a promover:
 - a) a harmonização com a legislação nacional e com normas internacionais para permitir a

interoperabilidade técnica e jurisdicional dos sistemas e das aplicações desenvolvidas e implementadas no País;

b) a adoção de instrumentos regulatórios que promovam a inovação responsável, como ambientes regulatórios experimentais (sandboxes regulatórios), autorregulação e certificações de boas práticas e governança;

VI – celebrar, a qualquer momento, compromisso com agentes de IA para eliminar irregularidade, incerteza jurídica ou situação contenciosa no âmbito de processos administrativos, de acordo com o previsto no Decreto-Lei no 4.657, de 4 de setembro de 1942 (Lei de Introdução às Normas do Direito Brasileiro).

PROPOSTA

Art. 48. Compete à autoridade setorial:

I – exercer competência regulatória, fiscalizatória e sancionatória, conforme sua esfera de competência outorgada por lei, para desenvolvimento, implementação e uso de sistemas de IA;

II – expedir regras específicas para a aplicação de IA, incluindo aspectos relacionados a atividades de alto risco, observadas as normas gerais expedidas pela autoridade competente;

III – promover e incentivar o disposto no Capítulo VI desta Lei para sistemas de IA que se inserem em sua esfera de competência outorgada por lei;

IV – quanto à sua esfera de competência outorgada por lei, incentivar a adoção de padrões, melhores práticas e modelos de certificação e acreditação reconhecidos internacionalmente;

V – supervisionar as medidas de governança adequadas a cada aplicação ou uso de sistemas de IA que classifique como de alto risco, de forma a promover:

a) a harmonização com a legislação nacional e com normas internacionais para permitir a interoperabilidade técnica e jurisdicional dos sistemas e das aplicações desenvolvidas e implementadas no País;

b) a adoção de instrumentos regulatórios que promovam a inovação responsável, como ambientes regulatórios experimentais (sandboxes regulatórios), autorregulação e certificações de boas práticas e governança;

VI – celebrar, a qualquer momento, compromisso com agentes de IA para eliminar irregularidade, incerteza jurídica ou situação contenciosa no âmbito de processos administrativos, de acordo com o previsto no Decreto-Lei no 4.657, de 4 de setembro de 1942 (Lei de Introdução às Normas do Direito Brasileiro).

VII - realizar auditorias regulares, no que se refere ao desenvolvimento de padrões de dados e metadados no combate a vieses e violações de direitos humanos, ao longo do ciclo de vida

dos dados;

VIII - regulamentar os casos em que a realização ou auditoria da avaliação de impacto será necessariamente conduzida por profissional ou equipe de profissionais externos ao fornecedor;

IX - instituir, regulamentar e supervisionar ecossistemas de dados setoriais, bem como estabelecer padrões e requisitos de interoperabilidade, visando à integração, compartilhamento seguro e uso ético das informações entre entidades públicas e privadas, em conformidade com a legislação aplicável e com o interesse público.

JUSTIFICATIVA

As mudanças propostas visam o fortalecimento da autoridade competente no sistema de enforcement de Inteligência artificial. Isso ocorre pois a redação atual cria inconsistências normativas e fiscalizatórias, levando a um cenário de provável insegurança jurídica. Uma das soluções propostas é incluir uma competência de garantia de consistência normativa. Nesse sentido, uma das missões institucionais da autoridade competente é garantir que as normas jurídicas sejam harmônicas, não colidentes e incapazes de produzir antinomias. Sem essas competências, corre-se o risco de uma inflação normativa e a introdução de normas jurídicas antinômicas, que acentuam a insegurança jurídica por produzirem conflitos de interpretação dentro do ordenamento jurídico.

No desenho atual do Sistema Nacional de Regulação e Governança de Inteligência Artificial (SIA), há conflito de competências entre autoridades setoriais e competentes. As mudanças sugeridas fortalecem um procedimento de construção normativa e fiscalização que impede tais conflitos ao mesmo tempo que permitem a colaboração delas.

Também foram incluídas disposições acerca das atribuições das autoridades competentes que tentam espelhar a lógica de certas disposições da Lei Nº 13.709 Lei Geral de Proteção de Dados Pessoais (LGPD). Essas disposições envolvem competências de orientação e conscientização da população sobre direitos; promoção de padrões de garantia de direitos; participação da sociedade civil, publicidades de sistemas de IA e na construção de uma política nacional de inteligência artificial.

REDAÇÃO ATUAL

Art. 47. Na qualidade de regulador residual, a autoridade competente exercerá competência normativa, regulatória, fiscalizatória e sancionatória plena para desenvolvimento, implementação e uso de sistemas de IA para atividades econômicas em que não haja órgão ou ente regulador setorial específico.

[...]

Art. 46. Na qualidade de coordenadora do SIA e sem prejuízo das competências previstas na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), cabe à autoridade competente:

I – atuar na representação do Brasil perante organismos internacionais de IA, sob a coordenação do Poder Executivo;

II – expedir, em colaboração com os demais integrantes do SIA, normas vinculantes de caráter geral sobre os seguintes temas:

a) forma e requisitos das informações a serem publicizadas sobre a utilização de sistemas de IA, respeitados os segredos industrial e comercial;

b) procedimentos e requisitos para elaboração da avaliação de impacto algorítmico;

c) procedimentos para a comunicação de incidentes graves, notadamente quando afetarem direitos fundamentais;

III – expedir regras gerais sobre IA no País, dando suporte aos órgãos setoriais, aos quais cabe a edição de regras específicas;

IV – celebrar com os integrantes do SIA acordos regulatórios para definir regras e procedimentos específicos de coordenação de competências;

V – expedir orientações normativas gerais sobre certificados e acreditação de organismos de certificação com o objetivo de incentivar e assegurar as melhores práticas de governança ao longo de todo o ciclo de vida de sistemas de IA;

VI – incentivar a adoção de padrões, melhores práticas e certificações reconhecidas internacionalmente;

VII – receber e tratar denúncias anônimas, estabelecendo mecanismos de reserva de identidade do denunciante;

VIII – elaborar relatórios anuais acerca de suas atividades.

Parágrafo único. Nos ambientes regulatórios experimentais (sandboxes regulatórios) que envolvam sistemas de IA, conduzidos por autoridades setoriais, a autoridade competente será científica, podendo manifestar-se quanto ao cumprimento das finalidades e dos princípios desta Lei.

[...]

Art. 49. Cabe à autoridade competente:

I – zelar pela proteção a direitos fundamentais e a demais direitos afetados pela utilização de sistemas de IA;

II – promover e incentivar o disposto no Capítulo VI desta Lei;

III – promover ações de cooperação com autoridades de proteção e de fomento ao desenvolvimento e à utilização dos sistemas de IA de outros países, de natureza internacional ou transnacional;

IV – solicitar, a qualquer momento, às entidades do poder público que desenvolvam ou utilizem sistemas de IA, informe específico sobre o âmbito e a natureza dos dados e demais detalhes do tratamento realizado, com a possibilidade de emitir parecer técnico complementar para garantir o cumprimento desta Lei;

V – celebrar, em conjunto com as autoridades setoriais, a qualquer momento, compromisso com agentes de IA para eliminar irregularidade, incerteza jurídica ou situação contenciosa no âmbito de processos administrativos, de acordo com o previsto no Decreto-Lei nº 4.657, de 4 de setembro de 1942 (Lei de Introdução às Normas do Direito Brasileiro);

VI – elaborar relatórios anuais acerca de suas atividades;

VII – realizar ou determinar auditorias de sistemas de IA de alto risco ou que produzam efeitos jurídicos relevantes quando necessárias para a aferição de conformidade com esta Lei, garantido o tratamento confidencial das informações, em atenção aos segredos comercial e industrial;

VIII – credenciar instituições, mediante critérios estabelecidos em regulamento sujeito a consulta pública, para acesso a dados para fins de auditorias e pesquisa, garantida a confidencialidade das informações, em atenção aos segredos comercial e industrial;

IX – credenciar instituições de pesquisa, mediante critérios estabelecidos em regulamento su-

jeito a consulta pública, para acesso a dados para fins de pesquisa, observados os segredos comercial e industrial, a anonimização e a proteção de dados pessoais, conforme a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais).

§ 1º Tanto a autoridade competente quanto eventuais entidades por ela credenciadas para a realização de auditoria e para fins de pesquisa devem cumprir requisitos de segurança e confidencialidade das informações e de proteção de dados pessoais, nos termos da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), em atenção aos segredos comercial e industrial.

§ 2º A autoridade competente, em conjunto com as autoridades setoriais, poderá realizar investigações sobre os sistemas de IA de alto risco, em caso de suspeita de violação aos princípios, direitos e deveres previstos nesta Lei ou na legislação setorial aplicável.

§ 3º Os órgãos e as entidades integrantes do SIA devem comunicar imediatamente ao Conselho Administrativo de Defesa Econômica (Cade) quaisquer informações identificadas no decurso das atividades de fiscalização que possam ser de interesse para a aplicação da Lei nº 12.529, de 30 de novembro de 2011 (Lei de Defesa da Concorrência).

§ 4º No exercício das suas atribuições e sempre no limite do que for pertinente e necessário à apuração de indícios concretos de infrações à ordem econômica, o Cade poderá ordenar aos desenvolvedores que seja concedido acesso aos conjuntos de dados de treino, validação e teste utilizados para o desenvolvimento dos sistemas de IA de alto risco.

[...]

Art. 16. A regulamentação da lista e a classificação de novas aplicações de sistemas de IA de alto risco serão precedidas de procedimento que garanta participação social e de análise de impacto regulatório, cabendo:

I – à autoridade competente, como coordenadora do SIA, garantir a aplicação harmônica desta Lei, devendo:

- a) expedir orientações normativas gerais em relação aos impactos dos sistemas de IA sobre os direitos e as liberdades fundamentais ou que produzam efeitos jurídicos relevantes;
- b) publicar a lista consolidada de todos os sistemas de alto risco definidos pelas autoridades setoriais;

II – às autoridades setoriais, no âmbito de suas atribuições e em caráter prevalente, dispor sobre os aspectos técnicos e específicos de aplicações de IA no mercado regulado, devendo:

- a) estabelecer listas sobre hipóteses classificadas ou não classificadas como de alto risco dentro das finalidades e contextos definidos no art. 14;
- b) estabelecer, com precisão, o rol de sistemas de alto risco desta Lei;
- c) receber e analisar as avaliações de impacto algorítmico;
- d) indicar, em lista, casos de utilização de sistemas ou aplicações de sistemas de IA de alto risco ou não.

§ 1º A autoridade competente e as autoridades setoriais deverão considerar o estado da arte do desenvolvimento tecnológico e a evolução e a harmonização das boas práticas setoriais e não setoriais para fins de monitoramento e reclassificação contínua dos sistemas de IA de alto risco.

§ 2º O desenvolvedor e o aplicador que considerar que o sistema de IA não se enquadra na

classificação de alto risco poderá apresentar petição fundamentada às autoridades setoriais juntamente com a sua avaliação preliminar, nos termos de regulamento.

§ 3º Os distribuidores deverão assegurar que o sistema de IA cumpra as medidas de governança previstas nesta Lei antes de ser colocado em circulação no mercado.

§ 4º A autoridade competente e as autoridades setoriais poderão acreditar organismos de avaliação de conformidade que ofereçam aos agentes de IA serviços de identificação e classificação de risco do uso de sistemas de IA, em conformidade com normas técnicas nacionais e internacionais aplicáveis.

§ 5º Na classificação de novas aplicações de sistemas de IA de alto risco, as autoridades setoriais deverão:

I – indicar de modo expresso suas consequências jurídicas e administrativas e as condições para que a regularização ocorra de modo proporcional e equânime, não se podendo impor aos sujeitos atingidos ônus ou perdas que, em função das peculiaridades do caso, sejam anormais ou excessivos;

II – considerar os obstáculos e as dificuldades reais dos agentes de IA e as exigências das políticas públicas a seu cargo, sem prejuízo dos direitos das pessoas e dos grupos afetados;

III – prever regime de transição para que novas obrigações e deveres sejam cumpridos de forma proporcional, equânime e eficiente e sem prejuízo dos interesses das pessoas e dos grupos afetados por sistemas de IA.

§ 6º O procedimento referido no caput deste artigo deverá oportunizar a manifestação dos setores econômicos produtivos afetados.

PROPOSTA

Art. 47. Na qualidade de regulador residual, a autoridade competente exercerá competência normativa, regulatória, fiscalizatória e sancionatória plena para desenvolvimento, implementação e uso de sistemas de IA para atividades econômicas em que não haja órgão ou ente regulador setorial específico.

[...]

Art. 46. Na qualidade de coordenadora do SIA e sem prejuízo das competências previstas na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), cabe à autoridade competente:

I – atuar na representação do Brasil perante organismos internacionais de IA, sob a coordenação do Poder Executivo;

II – expedir, em colaboração com os demais integrantes do SIA, normas vinculantes de caráter geral sobre os seguintes temas **incluindo, mas não se limitando a:**

a) forma e requisitos das informações a serem publicizadas sobre a utilização de sistemas de IA, respeitados os segredos industrial e comercial;

b) procedimentos e requisitos para elaboração da avaliação de impacto algorítmico;

c) procedimentos para a comunicação de incidentes graves, notadamente quando afetarem

direitos fundamentais;

d) procedimentos voltados à promoção e efetivação de direitos fundamentais de pessoas afetadas por sistemas de IA;

e) requisitos mínimos de transparência, explicabilidade e auditabilidade dos sistemas de IA, com vistas a garantir o direito à informação e a prevenção de riscos aos direitos fundamentais;

III – expedir regras gerais sobre IA no País, dando suporte aos órgãos setoriais, aos quais cabe a edição de regras específicas;

IV - definir os parâmetros e as diretrizes normativas que deverão ser observadas pelas autoridades setoriais na edição de regulamentações específicas, com vistas a garantir a consistência normativa;

V – celebrar com os integrantes do SIA acordos regulatórios para definir regras e procedimentos específicos de coordenação de competências;

V – expedir orientações normativas gerais sobre certificados e acreditação de organismos de certificação com o objetivo de incentivar e assegurar as melhores práticas de governança ao longo de todo o ciclo de vida de sistemas de IA;

VI – incentivar a adoção de padrões, melhores práticas e certificações reconhecidas internacionalmente;

VII – receber e tratar denúncias anônimas, estabelecendo mecanismos de reserva de identidade do denunciante;

VIII – elaborar relatórios anuais acerca de suas atividades.

Parágrafo único. Nos ambientes regulatórios experimentais (sandboxes regulatórios) que envolvam sistemas de IA, conduzidos por autoridades setoriais, a autoridade competente será científica, podendo manifestar-se quanto ao cumprimento das finalidades e dos princípios desta Lei.

[...]

Art. 49. Cabe à autoridade competente:

I – zelar pela proteção a direitos fundamentais e a demais direitos afetados pela utilização de sistemas de IA;

II – promover e incentivar o disposto no Capítulo VI desta Lei;

III – promover ações de cooperação com autoridades de proteção e de fomento ao desenvolvimento e à utilização dos sistemas de IA de outros países, de natureza internacional ou transnacional;

IV – solicitar, a qualquer momento, às entidades do poder público que desenvolvam ou utilizem sistemas de IA, informe específico sobre o âmbito e a natureza dos dados e demais detalhes do tratamento realizado, com a possibilidade de emitir parecer técnico complementar para garantir o cumprimento desta Lei;

V – celebrar, em conjunto com as autoridades setoriais, a qualquer momento, compromisso com agentes de IA para eliminar irregularidade, incerteza jurídica ou situação contenciosa no âmbito de processos administrativos, de acordo com o previsto no Decreto-Lei nº 4.657, de 4 de setembro de 1942 (Lei de Introdução às Normas do Direito Brasileiro);

VI – elaborar relatórios anuais acerca de suas atividades;

VII – realizar ou determinar auditorias de sistemas de IA de alto risco ou que produzam efeitos jurídicos relevantes quando necessárias para a aferição de conformidade com esta Lei, garantido o tratamento confidencial das informações, em atenção aos segredos comercial e industrial;

VIII – credenciar instituições, mediante critérios estabelecidos em regulamento sujeito a consulta pública, para acesso a dados para fins de auditorias e pesquisa, garantida a confidencialidade das informações, em atenção aos segredos comercial e industrial;

IX – credenciar instituições de pesquisa, mediante critérios estabelecidos em regulamento sujeito a consulta pública, para acesso a dados para fins de pesquisa, observados os segredos comercial e industrial, a anonimização e a proteção de dados pessoais, conforme a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais).

X – editar regulamentos gerais sobre o desenvolvimento e a utilização de sistemas de inteligência artificial, coordenando a atuação normativa das autoridades setoriais, que deverão se orientar por seus parâmetros e diretrizes.

XI- contribuir para a elaboração de diretrizes para a Política Nacional de Inteligência Artificial;

XII - promover o conhecimento das normas e das políticas públicas sobre Inteligência Artificial entre a população brasileira;

XIII - estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle das pessoas afetadas por sistemas de inteligência artificial, os quais deverão levar em consideração as especificidades de tais sistemas;

XIV - dispor sobre as formas de publicidade de sistemas de inteligência artificial de alto risco, respeitados os segredos comercial e industrial;

XV - ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento;

XVI - deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação desta Lei, as suas competências e os casos omissos;

§ 1º Tanto a autoridade competente quanto eventuais entidades por ela credenciadas para a realização de auditoria e para fins de pesquisa devem cumprir requisitos de segurança e confidencialidade das informações e de proteção de dados pessoais, nos termos da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), em atenção aos segredos comercial e industrial.

§ 2º A autoridade competente, em conjunto com as autoridades setoriais, poderá realizar investigações sobre os sistemas de IA de alto risco, em caso de suspeita de violação aos princípios, direitos e deveres previstos nesta Lei ou na legislação setorial aplicável.

§ 3º Os órgãos e as entidades integrantes do SIA devem comunicar imediatamente ao Conselho Administrativo de Defesa Econômica (Cade) quaisquer informações identificadas no decurso das atividades de fiscalização que possam ser de interesse para a aplicação da Lei nº 12.529, de 30 de novembro de 2011 (Lei de Defesa da Concorrência).

§ 4º No exercício das suas atribuições e sempre no limite do que for pertinente e necessário à apuração de indícios concretos de infrações à ordem econômica, o Cade poderá ordenar aos desenvolvedores que seja concedido acesso aos conjuntos de dados de treino, validação e teste

utilizados para o desenvolvimento dos sistemas de IA de alto risco.

§ 5º Cabe à autoridade competente a coordenação normativa do sistema regulatório aplicável aos sistemas de inteligência artificial, inclusive por meio da edição de regulamentos gerais. As autoridades setoriais somente poderão editar regulamentações específicas com base nos parâmetros e diretrizes previamente estabelecidos por essa autoridade, de forma a assegurar a consistência normativa e segurança jurídica.

§ 6º A autoridade competente terá prioridade na instauração de processos de fiscalização e poderá convidar as autoridades setoriais para participar das investigações, sempre que entender necessário, observadas as respectivas competências legais.

§ 7º autoridade competente poderá revisar, de ofício ou mediante provocação, a classificação de lista ou sistema de inteligência artificial como de alto risco realizada por autoridades setoriais, assegurado o contraditório e a ampla defesa ao agente de IA envolvido.

§ 8º Os regulamentos e as normas editados pela autoridade competente devem ser precedidos de consulta e audiência públicas, bem como de análises de impacto regulatório.

[...]

Art. 16. A regulamentação da lista e a classificação de novas aplicações de sistemas de IA de alto risco serão precedidas de procedimento que garanta participação social e de análise de impacto regulatório, cabendo:

I – à autoridade competente, como coordenadora do SIA, garantir a aplicação harmônica desta Lei, devendo:

a) expedir orientações normativas gerais em relação aos impactos dos sistemas de IA sobre os direitos e as liberdades fundamentais ou que produzam efeitos jurídicos relevantes;

b) publicar a lista consolidada de todos os sistemas de alto risco definidos pelas autoridades setoriais;

c) revisar, de ofício ou mediante provocação, a classificação de lista ou de sistema de inteligência artificial como de alto risco realizada pelas autoridades setoriais.

II – às autoridades setoriais, no âmbito de suas atribuições e em caráter prevalente, dispor sobre os aspectos técnicos e específicos de aplicações de IA no mercado regulado, devendo:

a) estabelecer listas sobre hipóteses classificadas ou não classificadas como de alto risco dentro das finalidades e contextos definidos no art. 14;

b) estabelecer, com precisão, o rol de sistemas de alto risco desta Lei;

c) receber e analisar as avaliações de impacto algorítmico;

d) indicar, em lista, casos de utilização de sistemas ou aplicações de sistemas de IA de alto risco ou não.

§ 1º A autoridade competente e as autoridades setoriais deverão considerar o estado da arte do desenvolvimento tecnológico e a evolução e a harmonização das boas práticas setoriais e não setoriais para fins de monitoramento e reclassificação contínua dos sistemas de IA de alto risco.

§ 2º O desenvolvedor e o aplicador que considerar que o sistema de IA não se enquadra na classificação de alto risco poderá apresentar petição fundamentada às autoridades setoriais jun-

tamente com a sua avaliação preliminar, nos termos de regulamento.

§ 3º Os distribuidores deverão assegurar que o sistema de IA cumpra as medidas de governança previstas nesta Lei antes de ser colocado em circulação no mercado.

§ 4º A autoridade competente e as autoridades setoriais poderão acreditar organismos de avaliação de conformidade que ofereçam aos agentes de IA serviços de identificação e classificação de risco do uso de sistemas de IA, em conformidade com normas técnicas nacionais e internacionais aplicáveis.

§ 5º Na classificação de novas aplicações de sistemas de IA de alto risco, as autoridades setoriais deverão:

I – indicar de modo expresse suas consequências jurídicas e administrativas e as condições para que a regularização ocorra de modo proporcional e equânime, não se podendo impor aos sujeitos atingidos ônus ou perdas que, em função das peculiaridades do caso, sejam anormais ou excessivos;

II – considerar os obstáculos e as dificuldades reais dos agentes de IA e as exigências das políticas públicas a seu cargo, sem prejuízo dos direitos das pessoas e dos grupos afetados;

III – prever regime de transição para que novas obrigações e deveres sejam cumpridos de forma proporcional, equânime e eficiente e sem prejuízo dos interesses das pessoas e dos grupos afetados por sistemas de IA.

§ 6º O procedimento referido no caput deste artigo deverá oportunizar a manifestação dos setores econômicos produtivos afetados.

JUSTIFICATIVA

Um dos elementos principais do Sistema Brasileiro de Inteligência Artificial (SIA) é o grau de coordenação e cooperação institucional entre agências setoriais e a autoridade competente por sua coordenação. Considerando que as autoridades setoriais possuem expertise técnica em seus setores regulados (por exemplo: a Anatel tem competência sobre assuntos setoriais de telecomunicações, ao passo que Anvisa tem competência sobre assuntos setoriais de saúde pública), é necessário criar obrigações de diálogo e cooperação institucional, incluindo a sinalização, para autoridade competente, de sistemas de IA que apresentam alto risco.

Ainda conforme mudanças no fortalecimento da autoridade competente, foram propostas mudanças para harmonizar a relação entre autoridade competente e autoridades setoriais. Também foi incluída a necessidade das autoridades setoriais de realizarem relatórios anuais sobre sua atividade como forma de tornar a gestão mais transparente e eficiente. Com a produção de relatórios anuais é possível avaliar a atuação de tais autoridades e propor mudanças no sentido de otimizar processos e aprimorar a eficiência da produção normativa e fiscalização.

REDAÇÃO ATUAL

Art. 48. Compete à autoridade setorial:

I – exercer competência regulatória, fiscalizatória e sancionatória, conforme sua esfera de competência outorgada por lei, para desenvolvimento, implementação e uso de sistemas de IA;

II – expedir regras específicas para a aplicação de IA, incluindo aspectos relacionados a atividades de alto risco, observadas as normas gerais expedidas pela autoridade competente;

III – promover e incentivar o disposto no Capítulo VI desta Lei para sistemas de IA que se inserem em sua esfera de competência outorgada por lei;

IV – quanto à sua esfera de competência outorgada por lei, incentivar a adoção de padrões, melhores práticas e modelos de certificação e acreditação reconhecidos internacionalmente;

V – supervisionar as medidas de governança adequadas a cada aplicação ou uso de sistemas de IA que classifique como de alto risco, de forma a promover:

a) a harmonização com a legislação nacional e com normas internacionais para permitir a interoperabilidade técnica e jurisdicional dos sistemas e das aplicações desenvolvidas e implementadas no País;

b) a adoção de instrumentos regulatórios que promovam a inovação responsável, como ambientes regulatórios experimentais (sandboxes regulatórios), autorregulação e certificações de boas práticas e governança;

VI – celebrar, a qualquer momento, compromisso com agentes de IA para eliminar irregularidade, incerteza jurídica ou situação contenciosa no âmbito de processos administrativos, de acordo com o previsto no Decreto-Lei nº 4.657, de 4 de setembro de 1942 (Lei de Introdução às Normas do Direito Brasileiro).

Art. 48. Compete à autoridade setorial:

I – exercer competência regulatória, fiscalizatória e sancionatória, conforme sua esfera de competência outorgada por lei, para desenvolvimento, implementação e uso de sistemas de IA;

II – expedir regras específicas para a aplicação de IA, incluindo aspectos relacionados a atividades de alto risco, observadas as normas gerais expedidas pela autoridade competente;

III – promover e incentivar o disposto no Capítulo VI desta Lei para sistemas de IA que se inserem em sua esfera de competência outorgada por lei;

IV – quanto à sua esfera de competência outorgada por lei, incentivar a adoção de padrões, melhores práticas e modelos de certificação e acreditação reconhecidos internacionalmente;

V – supervisionar as medidas de governança adequadas a cada aplicação ou uso de sistemas de IA que classifique como de alto risco, de forma a promover:

a) a harmonização com a legislação nacional e com normas internacionais para permitir a interoperabilidade técnica e jurisdicional dos sistemas e das aplicações desenvolvidas e implementadas no País;

b) a adoção de instrumentos regulatórios que promovam a inovação responsável, como ambientes regulatórios experimentais (sandboxes regulatórios), autorregulação e certificações de boas práticas e governança;

VI – celebrar, a qualquer momento, compromisso com agentes de IA para eliminar irregularidade, incerteza jurídica ou situação contenciosa no âmbito de processos administrativos, de acordo com o previsto no Decreto-Lei nº 4.657, de 4 de setembro de 1942 (Lei de Introdução às Normas do Direito Brasileiro).

IX – encaminhar à autoridade competente as listas de sistemas de IA classificadas como de alto risco, passíveis de revisão ou consolidação em lista única nacional.

VIII – elaborar relatórios anuais acerca de suas atividades, disponibilizados em formato acessível na Internet.

JUSTIFICATIVA

Na mesma linha da Contribuição do Conselho Administrativo de Defesa Econômica (Cade), entendemos que a presença da Autoridade Concorrencial no SIA é de suma importância para garantir maior segurança jurídica para atuações institucionais conjuntas das entidades, bem como para ampliar o leque de oportunidades de investigação coordenada, melhorando, assim, o enforcement do conjunto de obrigações e deveres dispostos na Lei.

Como garantidor da livre concorrência e do bem estar do consumidor, a presença do Cade como entidade integrante do SIA é extremamente necessária. A expertise técnica da Autarquia para atuar em diversos mercados relevantes pode contribuir na fiscalização e monitoramento do uso da IA por diferentes agentes em diferentes mercados. Além disso, o Cade se mostra um ator potencial no trabalho de advocacy feito pelo Executivo Federal, sendo capaz de incentivar e promover o uso consciente da IA em conformidade com os fundamentos da ordem econômica nacional.

No texto atual do PL, o Cade somente é mencionado no § 3º e 4º do art. 49 e, posteriormente, no art. 52º caput e parágrafo único. A primeira menção dispõe que os órgãos e as entidades integrantes do SIA devem, imediatamente, comunicar o Cade sobre informações que podem ser submetidas à aplicação da Lei nº 12.529/11, enquanto a segunda prevê que, no exercício das suas atribuições e nos limites da sua competência, o Cade pode ordenar que seja concedido acesso aos conjuntos de dados de treino, validação e teste utilizados para o desenvolvimento dos sistemas de IA de alto risco pelos desenvolvedores. O mesmo texto é repetido no art. 52º caput e parágrafo único.

Nota-se, entretanto, que o PL não especifica como se dará esse acesso ou o compartilhamento desses dados, isto é, deverá ser respeitado algum protocolo específico de interoperabilidade? Como será feita a coordenação das ações de supervisão e fiscalização dessas informações pelo SIA e pelo Cade? Entendemos, pois, que o Texto poderia conter dispositivos que conferissem mais transparência e clareza sobre esse processo.

Há, portanto, duas lacunas no texto do PL em termos de questões concorrenciais: a primeira, de natureza institucional (ausência do Cade no SIA) e a segunda, de natureza procedimental (falta de orientações sobre o compartilhamento de dados e informações entre o CADE e o SIA). Portanto, conclui-se pela importância da presença do Cade como entidade integrante do SIA, bem como pela necessidade de explicar e detalhar o funcionamento dos instrumentos de cooperação dos demais agentes que integram o SIA e o Cade.

REDAÇÃO ATUAL

Art. 45. O Poder Executivo é autorizado a estabelecer o Sistema Nacional de Regulação e Governança de Inteligência Artificial (SIA).

§ 1º Integram o SIA:

I – a Autoridade Nacional de Proteção de Dados (ANPD), autoridade competente que coordenará o SIA;

II – as autoridades setoriais;

III – o Conselho Permanente de Cooperação Regulatória de Inteligência Artificial (Cria), observado e limitado ao disposto na Seção IV deste Capítulo;

IV – o Comitê de Especialistas e Cientistas de Inteligência Artificial (Cecia), observado e limitado ao disposto na Seção V deste Capítulo.

§ 2º Ato do Poder Executivo federal definirá lista dos órgãos e entidades que irão integrar o SIA, em conformidade com os incisos II, III e IV do § 1º deste artigo.

§ 3º O SIA tem por objetivos e fundamentos:

I – valorizar e reforçar as competências regulatória, sancionatória e normativa das autoridades setoriais em harmonia com as competências correlatas gerais da autoridade competente que coordena o SIA; e

II – buscar a harmonização e a colaboração com órgãos reguladores de temas transversais.

PROPOSTA

Art. 45. O Poder Executivo é autorizado a estabelecer o Sistema Nacional de Regulação e Governança de Inteligência Artificial (SIA).

§ 1º Integram o SIA:

I – a Autoridade Nacional de Proteção de Dados (ANPD), autoridade competente que coordenará o SIA;

II – as autoridades e entidades reguladoras, quais sejam:

a) Órgãos e entidades estatais de regulação setorial;

b) O Conselho Administrativo de Defesa Econômica (Cade);

III – o Conselho Permanente de Cooperação Regulatória de Inteligência Artificial (Cria), observado e limitado ao disposto na Seção IV deste Capítulo;

IV – o Comitê de Especialistas e Cientistas de Inteligência Artificial (Cecia), observado e limitado ao disposto na Seção V deste Capítulo.

§ 2º Ato do Poder Executivo federal definirá lista dos órgãos e entidades que irão integrar o SIA, em conformidade com os incisos II, III e IV do § 1º deste artigo.

§ 3º O SIA tem por objetivos e fundamentos:

I – valorizar e reforçar as competências regulatória, sancionatória e normativa das autoridades setoriais em harmonia com as competências correlatas gerais da autoridade competente que coordena o SIA; e

II – buscar a harmonização e a colaboração com órgãos reguladores de temas transversais.

§ 4º As entidades reguladoras integrantes do SIA poderão realizar investigações conjuntas sobre os sistemas de IA de alto risco, em casos de suspeita de violação aos princípios, direitos e deveres previstos nesta Lei ou na legislação setorial aplicável.

I - As investigações conjuntas serão realizadas mediante solicitação de uma das entidades reguladoras envolvidas, com a concordância das demais, observando-se os procedimentos e as garantias previstas na legislação pertinente.

II - As entidades reguladoras poderão requerer o acesso remoto à documentação e aos conjuntos de dados de treinamento dos sistemas de IA de alto risco, desde que:

- a. o acesso seja necessário para a realização de investigações;
- b. o acesso seja proporcional, adequado e limitado ao mínimo necessário para a verificação da conformidade do sistema de IA;
- c. sejam adotadas medidas eficazes para proteger a confidencialidade, a integridade e a segurança dos dados acessados;
- d. sejam respeitados os direitos de propriedade intelectual e de proteção de dados pessoais.

JUSTIFICATIVA

A construção de regimes jurídicos experimentais, chamados de “Sandbox Regulatórios”, exige cuidado para contenção de uma potencial diluição da capacidade administrativa estatal. Esse instrumento serve para equilibrar a inovação e a proteção de direitos fundamentais, já estando previsto no Marco Legal das Startups (Lei Complementar 182/2021). O fato de haver uma seção inteira dedicada ao tema no capítulo X é extremamente positivo, assim como a previsão de condições especiais a agentes que querem desenvolver, treinar, validar e testar um sistema novo de IA, mediante o cumprimento de critérios e de limites previamente estabelecidos no PL. Entretanto, nota-se que não há qualquer menção à atuação do Cade nesse modelo regulatório experimental.

Conforme mencionado pelo Cade em sua contribuição, os Sandbox Regulatórios são vistos como uma abordagem utilizada para lidar com riscos concorrenciais de algoritmos de preços utilizados por pequenas e médias empresas, principalmente no contexto de algoritmos de precificação, uma vez que essas ferramentas podem, ao mesmo tempo, trazer benefícios pró competitivos significativos, mas também impor riscos concorrenciais por meio de técnicas de auto aprendizagem de máquina que ainda são pouco compreendidos pelas autoridades. Para a Autoridade Antitruste, isso poderia ser uma forma de testar o funcionamento e desenvolvimento de ferramentas de IA na prática, facilitando um estudo ex ante sobre possíveis impactos concorrenciais de tais técnicas no mercado.

Isso, pois, poderia se dar mediante o acompanhamento e a supervisão das entidades do SIA, em conjunto com demais autoridades, como o Cade, ANPD, bem como agências reguladoras cuja mercado relevante seja de seu interesse. Se um dos objetivos da regulação é impulsionar a inovação ao trazer mais segurança jurídica, quanto mais agentes responsáveis estiverem alinhados, maiores são as chances de se ter uma inovação segura e inclusiva.

Recomendamos, também, um cuidado com arranjos de flexibilização de normas jurídicas, que devem ser motivados, proporcionais e não podem produzir incentivo a aumento de riscos a liberdades e direitos fundamentais.

REDAÇÃO ATUAL

Art. 56. A autoridade competente e as autoridades setoriais que compõem o SIA regulamentarão os procedimentos para a solicitação e a autorização de funcionamento de sandboxes regulatórios, podendo limitar ou interromper o seu funcionamento e emitir recomendações, levando em consideração, entre outros aspectos, a preservação de direitos fundamentais e de direitos dos consumidores potencialmente afetados, a segurança e a proteção.

§ 1º As autoridades setoriais deverão proporcionar a micro e pequenas empresas, startups e Instituições Científica, Tecnológicas e de Inovação (ICTs) públicas e privadas acesso prioritário aos ambientes de testagem, na medida em que cumpram as condições de elegibilidade, os critérios de seleção e demais regulamentos.

§ 2º A autoridade competente e as autoridades setoriais poderão criar mecanismos para reduzir os custos regulatórios das entidades qualificadas na forma do § 1º do caput deste artigo.

PROPOSTA

Art. 56. A autoridade competente e as autoridades setoriais que compõem o SIA regulamentarão os procedimentos para a solicitação e a autorização de funcionamento de sandboxes regulatórios, podendo limitar ou interromper o seu funcionamento e emitir recomendações, levando em consideração, entre outros aspectos, a preservação de direitos fundamentais e de direitos dos consumidores potencialmente afetados, a segurança e a proteção e o impacto concorrencial das atividades econômicas correlatas.

§ 1º As autoridades setoriais deverão proporcionar condições especiais para a participação das micro e pequenas empresas, startups e Instituições Científica, Tecnológicas e de Inovação (ICTs) públicas e privadas, tais como:

I - acesso prioritário aos ambientes de testagem, na medida em que cumpram as condições de elegibilidade, os critérios de seleção e demais regulamentos;

§ 2º A autoridade competente e as autoridades setoriais poderão criar mecanismos para reduzir os custos regulatórios das entidades qualificadas na forma do § 1º do caput deste artigo.

§ 3º Dentre os critérios diferenciados que devem ser observados, tem-se o impacto concorrencial das atividades econômicas correlatas, o número de usuários afetados e a natureza das atividades econômicas exercidas.

§ 4º A flexibilização de normas jurídicas em sistemas de sandbox regulatório deve ser devidamente motivada e não pode ensejar o fomento a atividades que produzam maiores riscos a liberdades e direitos fundamentais.

JUSTIFICATIVA

A proposta de fortalecimento da Seção V, relativa ao Comitê de Especialistas e Cientistas de Inteligência Artificial (Cecia), visa garantir que sua atuação reflita as melhores práticas internacionais de governança digital, assegurando decisões transparentes, inclusivas e baseadas em evidências. O modelo multissetorial proposto inspira-se em mecanismos já consolidados, como o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPd) (ver seção IV), no Brasil, e em âmbito internacional no Painel Científico da ONU sobre IA proposto no Pacto Global Digital (ver par. 56.a; par. 57), no Órgão Consultivo de Alto Nível sobre Inteligência Artificial (High-Level Advisory Body on Artificial Intelligence), assim como no Advisory Forum e no Scientific Panel of Independent Experts do AI Act da União Europeia (ver art.67; art.68). Esses órgãos têm recorrido a processos participativos robustos, como consultas públicas e deep dives temáticos, reforçando a legitimidade das suas recomendações.

Além disso, a institucionalização de Grupos de Trabalho temáticos, a publicidade das reuniões e deliberações, e a integração com órgãos do Sistema Nacional de IA reforçam os princípios constitucionais da publicidade, eficiência e participação social, atendendo a demandas de documentos como a Declaração de São Luís (G20) (ver par. 15) e a Declaração Multissetorial do NetMundial+10 (ver tópico 2; tópico 3). Ainda, o estabelecimento das condições administrativas e financeiras para o funcionamento efetivo do CECIA alinha-se às demandas quanto à necessidade de garantir a sustentabilidade de iniciativas multissetoriais. Alinha-se, também, às disposições do AI Act da União Europeia referentes ao estabelecimento do Scientific Panel of Independent Experts, que conta com secretariado e recursos designados para o cumprimento de suas atividades, conforme o Regulamento de Execução 2025/454 da UE (ver art.6; art.7).

REDAÇÃO ATUAL

Seção V Do Comitê de Especialistas e Cientistas de Inteligência Artificial

Art. 54. É criado o Comitê de Especialistas e Cientistas de Inteligência Artificial (Cecia) com o objetivo de orientar e supervisionar técnica e cientificamente o desenvolvimento e a aplicação da IA de forma responsável, nos termos definidos por regulamento.

PROPOSTA

Art. 54. É criado o Comitê de Especialistas e Cientistas de Inteligência Artificial (Cecia) com objetivo de **assessorar técnica e cientificamente a formulação, o desenvolvimento, a implementação e a aplicação de sistemas de inteligência artificial no país, assegurando que ocorram de forma ética, responsável, segura e alinhada aos direitos fundamentais, nos termos definidos por regulamento.**

§1º O Cecia terá as seguintes competências:

I - Analisar e elaborar diretrizes sobre o desenvolvimento e a aplicação da inteligência artificial, observando a conformidade com direitos fundamentais;

II - Sugerir ações junto a ANPD e demais órgãos do SIA;

III - Colaborar para a promoção do diálogo entre órgãos da administração pública e entidades da sociedade civil, setor privado, comunidade técnico-científica e especialmente comunidades em situação de vulnerabilidade social;

IV - Elaborar estudos e realizar consultas e audiências públicas sobre o desenvolvimento e a aplicação da IA;

IV - Zelar pela transparência, pela publicidade e pela prestação de contas das suas atividades;

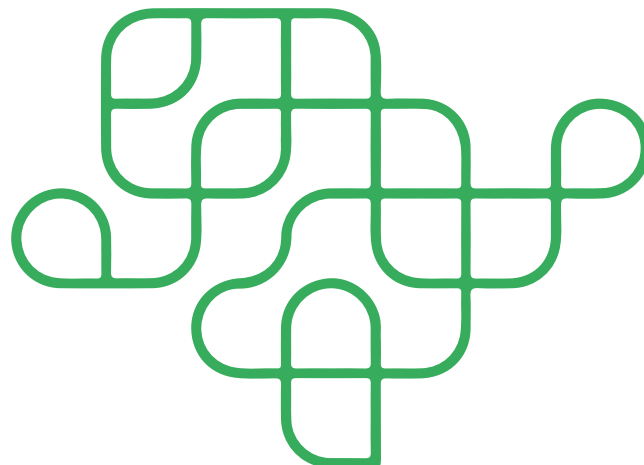
V - Disseminar o conhecimento sobre o desenvolvimento e a aplicação responsável da inteligência artificial à população em geral.

§2º A composição do Comitê de Especialistas e Cientistas de Inteligência Artificial (Cecia) deverá zelar pelo caráter multissetorial e equilibrada de representantes do poder público, da comunidade técnico-científica, do setor privado e da sociedade civil, observado a diversidade regional, de gênero e racial.

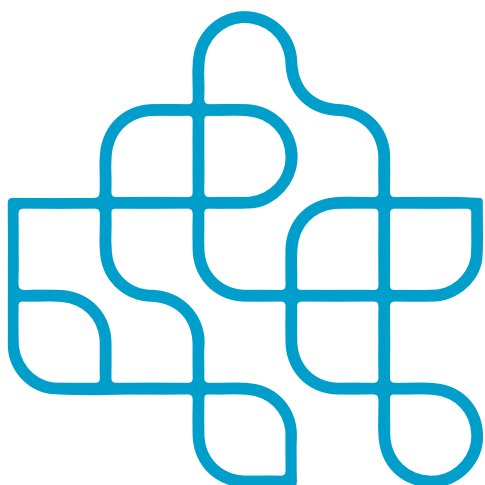
§3º O Comitê de Especialistas e Cientistas de Inteligência Artificial (Cecia) encaminhará regularmente suas deliberações, pareceres e recomendações aos órgãos do SIA e demais entidades públicas e privadas interessadas, com vistas à sua consideração e eventual incorporação nas respectivas políticas, planos e programas.

§4º O Comitê de Especialistas e Cientistas de Inteligência Artificial poderá editar regulamento interno para detalhar as normas complementares necessárias à aplicação desta Lei.

§ 5º. A Agência Nacional de Proteção de Dados (ANPD) deverá prover o suporte administrativo, técnico e orçamentário ao Comitê de Especialistas e Cientistas de Inteligência Artificial (CE-CIA), mediante a designação de secretariado permanente e a alocação de recursos necessários para o seu pleno funcionamento.



07. ATUAÇÃO DO PODER PÚBLICO



07. ATUAÇÃO DO PODER PÚBLICO

Governança de dados, segurança nacional, segurança pública, e sustentabilidade

JUSTIFICATIVA

O PBIA (ver Ação 28) prevê o estabelecimento de uma política de governança de dados para o Poder Público, institucionalizando o uso estratégico de dados e seu retorno para a sociedade. A Minuta da Política de Governança e Compartilhamento de Dados (ver art. 3.II; IV) dispõe sobre o uso estratégico de dados, pautando a gestão integral e o reuso de dados como princípios da governança de dados no setor público. A visão de uma governança de dados voltada à justiça social também remete ao trabalho do T20 Brasil e a abordagem de justiça de dados (ver Introdução; recomendação 2).

REDAÇÃO ATUAL

Art. 68. Constituem diretrizes para a atuação da União, dos Estados, do Distrito

Federal e dos Municípios no desenvolvimento da IA no Brasil:

I – estabelecimento de mecanismos de governança multiparticipativa, multissetorial transparente, colaborativa e democrática, com a participação do governo, do setor empresarial, do terceiro setor e da comunidade acadêmica, especialmente considerando os grupos vulneráveis;

II – promoção da confiança nas tecnologias de IA, com disseminação de informações e de conhecimento sobre seus usos éticos e responsáveis;

III – estímulo à capacitação e à preparação das pessoas para a reestruturação do mercado de trabalho;

IV – promoção da interoperabilidade entre sistemas de IA, inclusive entre os diferentes âmbitos federativos e diversos setores da sociedade, com decisões que busquem evitar a dependência tecnológica e propiciar a continuidade do emprego dos sistemas desenvolvidos ou contratados;

V – publicidade e disseminação de dados, de forma aberta, estruturada e segura;

VI – proteção ao meio ambiente e desenvolvimento sustentável;

VII – promoção da cooperação internacional, mediante estímulo ao compartilhamento do conhecimento sobre sistemas de IA, de modo a facilitar a interoperabilidade regulatória e tecnológica;

VIII – promoção de investimento em IA voltada para a solução dos problemas do País, promovendo seu desenvolvimento socioeconômico, cultural e ambiental, e para o desenvolvimento do sistema produtivo nacional e regional, prezando pela autonomia tecnológica do País e sua inserção e competitividade nos mercados interno e internacional.

PROPOSTA

Art. 68. Constituem diretrizes para a atuação da União, dos Estados, do Distrito

Federal e dos Municípios no desenvolvimento da IA no Brasil:

V - publicidade e disseminação de dados, de forma aberta, estruturada e segura, com adoção de licenças públicas e abertas que permitam o livre uso, reuso estratégico e redistribuição de dados de interesse público, visando ainda a interoperabilidade e compartilhamento eficiente de dados entre órgãos e entidades governamentais;

IX - promoção da justiça social e ambiental, garantindo o tratamento ético dos dados, observada a não discriminação, a promoção da cidadania, a inclusão social, digital e econômica, a responsabilidade, a equidade, a confiança, a veracidade e a proteção de grupos vulneráveis;

X - transparência e participação pública quanto à governança dos ecossistemas de dados;

XI - condução de esforços de interoperabilidade entre os sistemas e atores participantes;

XII - condução de esforços de interoperabilidade com parceiros de cooperação internacional, e em conjunto com órgãos de padronização nacionais e internacionais, facilitando a interoperabilidade e a cooperação internacional para governança de dados.

Direitos coletivos de acesso à informação

JUSTIFICATIVA

São expressivas as evidências de impactos ambientais, urbanos e sociais para a instalação de data centers, estruturas imprescindíveis para processamento de dados de IA. O PL 2338 traz em seu Capítulo X, Seção III, medidas importantes para sustentabilidade, mas falta ao texto elementos procedimentais para averiguação das garantias ambientais, além de medidas de transparência para controle social.

Tratam-se de medidas aderentes ao dever de transparência pública, previsto tanto na Constituição Federal, quanto na Lei de Acesso à Informação. Com isso, entidades públicas e privadas terão maior segurança jurídica na implementação de projetos no país, especialmente no setor de investimentos, que terão maior capacidade de avaliação técnica da viabilidade de empreendimentos.

Ademais, tais medidas são importantes para conter eventuais disputas entre municípios e estados para incorporação de data centers em seus territórios a partir de benefícios fiscais. Muitas vezes desmedidos, os incentivos à instalação de indústrias não consideram potenciais danos urbanos, ambientais e sociais ao território, sendo importante garantir procedimentos com transparência ativa e passiva. Isso traz como retorno a confiabilidade de novas soluções inovadoras e controle social do setor público e privado.

REDAÇÃO ATUAL

Inexistente

PROPOSTA

Art. 60-B: Os empreendimentos em data centers e infraestrutura para IA no Brasil devem garantir o direito do público de acesso a informações ambientais, urbanas e sociais que estejam em seu poder, sob seu controle ou custódia.

§1º Devem ser adotadas medidas de transparência ativa e passiva, nos termos da Lei de Acesso à Informação, para garantia de controle social a respeito de empreendimentos públicos sobre infraestrutura de IA.

§2º Empresas privadas que recebem fundos ou benefícios públicos, direta ou indiretamente, isenções tributárias ou que realizem funções ou serviços públicos, também devem adotar medidas de transparência ativa e passiva sobre informações ambientais, urbanas e sociais para implementação de empreendimentos e manutenção de data centers e infraestrutura de IA, nos termos da Lei de Acesso à Informação.

§3º Qualquer negativa de acesso deverá ser fundamentada, informando ao solicitante sobre o direito de impugnação e recurso para autoridade competente.

§4º O direito de peticionamento de acesso a informações ambientais, sociais e urbanas pode ser exercido por pessoas naturais e por associações que representam interesses coletivos e difusos.

§5º Por informações ambientais entende-se qualquer informação escrita, visual, sonora, eletrônica ou registrada em qualquer outro formato, relativa ao meio ambiente e seus elementos e aos recursos naturais, incluindo as informações relacionadas com os riscos ambientais e os possíveis impactos adversos associados que afetem ou possam afetar o meio ambiente e a saúde, bem como as relacionadas com a proteção e a gestão ambientais.

§6º As empresas de datacenters não poderão recusar a disponibilização de acesso a informações ambientais, incluindo os de energia e água, sob justificativa de segredo industrial ou segredo comercial, considerando o direito de toda pessoa a viver em um meio ambiente saudável e sustentável.

§ 7º O Poder Executivo poderá editar decreto de regulamentação sobre o direito coletivo de acesso a informações ambientais, urbanas e sociais, nos termos da lei.

JUSTIFICATIVA

Reforçar a obrigatoriedade de realizar Avaliação de Risco.

REDAÇÃO ATUAL

Art. 12. Antes de sua introdução e circulação no mercado, emprego ou utilização, o agente de IA poderá realizar avaliação preliminar para determinar o grau de risco do sistema, baseando-se nos critérios previstos neste Capítulo, de acordo com o estado da arte do desenvolvimento tecnológico.

PROPOSTA

Art. 54. É criado o Comitê de Especialistas e Cientistas de Inteligência Artificial (Cecia) com oArt. 12. Antes de sua introdução e circulação no mercado, emprego ou utilização, o agente de IA **deverá** realizar avaliação preliminar para determinar o grau de risco do sistema, baseando-se nos critérios previstos neste Capítulo, de acordo com o estado da arte do desenvolvimento tecnológico.

JUSTIFICATIVA

A utilização de sistemas de IA já traz danos a direitos de cidadãos brasileiros. O cenário pode ser ainda mais desafiador à medida que novos setores utilizam SIAs para desenvolvimento de produtos e serviços. Ainda que haja ganhos em inovação e produtividade, faz-se necessário estabelecer limites evidentes dos campos da vida pública e privada que devem ser limitados. Nesse sentido, a proposta busca fomentar uma proteção mais ampla à saúde física e mental, bem como à integridade financeira de famílias. A inclusão no dispositivo demonstra compromisso do Poder Público em uma regulação atenta às necessidades da população brasileira.

REDAÇÃO ATUAL

Art. 13. São vedados o desenvolvimento, a implementação e o uso de sistemas de IA:

I – com o propósito de:

a) instigar ou induzir o comportamento da pessoa natural ou de grupos de maneira que cause danos à saúde, à segurança ou a outros direitos fundamentais próprios ou de terceiros;

b) explorar quaisquer vulnerabilidades da pessoa natural ou de grupos com o objetivo ou o efeito de induzir o seu comportamento de maneira que cause danos à saúde, à segurança ou outros a direitos fundamentais próprios ou de terceiros;

(...)

d) possibilitar a produção ou disseminação ou facilitar a criação de material que caracterize ou represente abuso ou exploração sexual de crianças e adolescentes;

PROPOSTA

Art. 13. São vedados o desenvolvimento, a implementação e o uso de sistemas de IA:

I – com o propósito de:

a) instigar ou induzir o comportamento da pessoa natural ou de grupos de maneira que cause danos à saúde **física e mental**, à segurança ou a outros direitos fundamentais próprios ou de terceiros;

b) explorar quaisquer vulnerabilidades da pessoa natural ou de grupos com o objetivo ou o efeito de induzir o seu comportamento de maneira que cause danos à saúde, à segurança, **à integridade financeira** ou outros a direitos fundamentais próprios ou de terceiros;

(...)

d) possibilitar a produção ou disseminação ou facilitar a criação de material que caracterize ou represente abuso ou exploração sexual de crianças e adolescentes, **bem como danos a sua integridade física e mental**;

JUSTIFICATIVA

A aplicação de SIA na administração da justiça tem impactos profundos no devido processo legal, direito ao contraditório e ampla defesa, bem como acesso ao Poder Judiciário. Por conta disso, a proposta aponta como de alto risco sistemas aplicados nesse contexto. Vemos, hoje, uma utilização de diferentes ferramentas por juízes e servidores de tribunais, seja a partir da contratação de terceiros ou desenvolvimento de aplicações internas.

Ainda que importantes para a eficiência da justiça brasileira - com milhões de processos em curso - faz-se necessário delimitar limites para seu uso e medidas de transparência adequadas. Isso é especialmente relevante não apenas em sentenças, mas também decisões interlocutórias, despachos e demais procedimentos administrativos que possam influenciar nas fases de conhecimento e execução de processos judiciais. A proposta de redação acrescenta procedimentos administrativos e decisões para evidenciar a proteção ampla aos danos diante de uso de SIA no Poder Judiciário.

REDAÇÃO ATUAL

art. 14 VI – administração da justiça, no que se refere ao uso de sistemas que auxiliem autoridades judiciárias na investigação dos fatos e na aplicação da lei quando houver risco às liberdades individuais e ao Estado democrático de direito, excluindo-se os sistemas que auxiliem atos e atividades administrativas;

PROPOSTA

art. 14 VI – administração da justiça, no que se refere ao uso de sistemas que auxiliem autoridades judiciárias na investigação dos fatos, **procedimentos administrativos, decisões** e na aplicação da lei quando houver risco às liberdades individuais e ao Estado democrático de direito, excluindo-se os sistemas que auxiliem atos e atividades administrativas;

IA no judiciário precisaria entrar em contexto parecido com esse, mas considerando decisões judiciais, análise de recursos e redação de sentenças

JUSTIFICATIVA

Por se tratar de uma tecnologia com o potencial de afetar não somente o indivíduo, mas grupos ou até mesmo a população como um todo. É essencial garantir que os agentes envolvidos se responsabilizem pela transparência de seus processos, de forma ativa e passiva.

A avaliação de impacto algorítmico é um documento essencial para cumprir com os princípios de transparência e explicabilidade, bem como diligência devida e auditabilidade. Sendo assim, deve ser elaborado de forma clara e inteligível, sendo amplamente divulgado em canal específico.

No mais, considerando os direitos das pessoas e grupos afetados, deve existir um canal para contato que permita a manifestação, participação e oposição frente a decisões tomadas quanto à implementação dos sistemas de IA.

REDAÇÃO ATUAL

Art. 28. As conclusões da avaliação de impacto algorítmico serão públicas, observados os segredos industrial e comercial, nos termos de regulamento.

PROPOSTA

Art. 28. **A avaliação de impacto algorítmico será pública**, respeitados os segredos industrial e comercial, conforme definido em regulamento a ser estabelecido pela autoridade competente nos termos das diretrizes do Cria.

§ 1º. **A avaliação de impacto algorítmico deverá ser publicada pelo agente de inteligência artificial responsável, em canal acessível ao público, com informações claras, atualizadas e objetivas, inclusive para pessoas com deficiências. A publicação deverá observar as diretrizes de transparência definidas pela autoridade competente, nos termos do regulamento geral, e assegurar o respeito aos direitos das pessoas e grupos afetados.**

JUSTIFICATIVA

A redação atual do PL 2338/2023 apresenta lacunas no que se refere à prevenção de abusos estatais e à proteção efetiva de direitos fundamentais no contexto de segurança pública. Faltam mecanismos claros de responsabilização, transparência, controle social e participação pública nos processos decisórios que envolvem a adoção e o uso de sistemas de inteligência artificial por órgãos de segurança.

Essas lacunas dificultam a identificação e a mitigação de riscos, comprometem a prestação de contas e enfraquecem as garantias constitucionais de legalidade, proporcionalidade e não discriminação. A incorporação de salvaguardas específicas é necessária para assegurar que o uso dessas tecnologias ocorra dentro de parâmetros técnicos e jurídicos que respeitem os direitos humanos, a legislação vigente e os princípios do Estado Democrático de Direito.

REDAÇÃO ATUAL

Inclusão no art. 23

PROPOSTA

Art. 23-B. Em caso de violações de direitos decorrentes do uso de sistemas de IA por entes estatais em atividades de segurança pública, deve-se garantir:

- I - o direito à reparação integral da pessoa afetada, incluindo compensação moral e material;
- II - a responsabilização administrativa, civil e penal dos agentes responsáveis pela implantação, fiscalização ou o uso indevido dos sistemas;
- III - a investigação obrigatória e imediata pela corregedoria competente, com relatório público sobre o incidente.

Art. 23-C. Todos os sistemas de IA utilizados em segurança pública devem ser registrados em plataforma pública nacional, com as seguintes informações:

- I - órgão responsável pelo uso;
- II - fornecedor ou desenvolvedor da tecnologia;
- III - finalidade e base legal do uso;
- IV - eventuais avaliações de impacto algorítmico ou relatórios de auditoria;
- V - histórico de incidentes relacionados à tecnologia.

Art. 23-D. Os sistemas de utilizados por órgãos de segurança pública deverão estar sujeitos a fiscalização contínua pelos seguintes mecanismos:

- I - acesso garantido e periódico às Defensorias Públicas e ao Ministério Público sobre os dados e decisões automatizadas;
- II - relatório anual enviado ao Congresso Nacional sobre os impactos da IA na segurança pública.

blica, contendo indicadores de raça, gênero, região e classe social.

REDAÇÃO ATUAL

Art. 13 inclusão

PROPOSTA

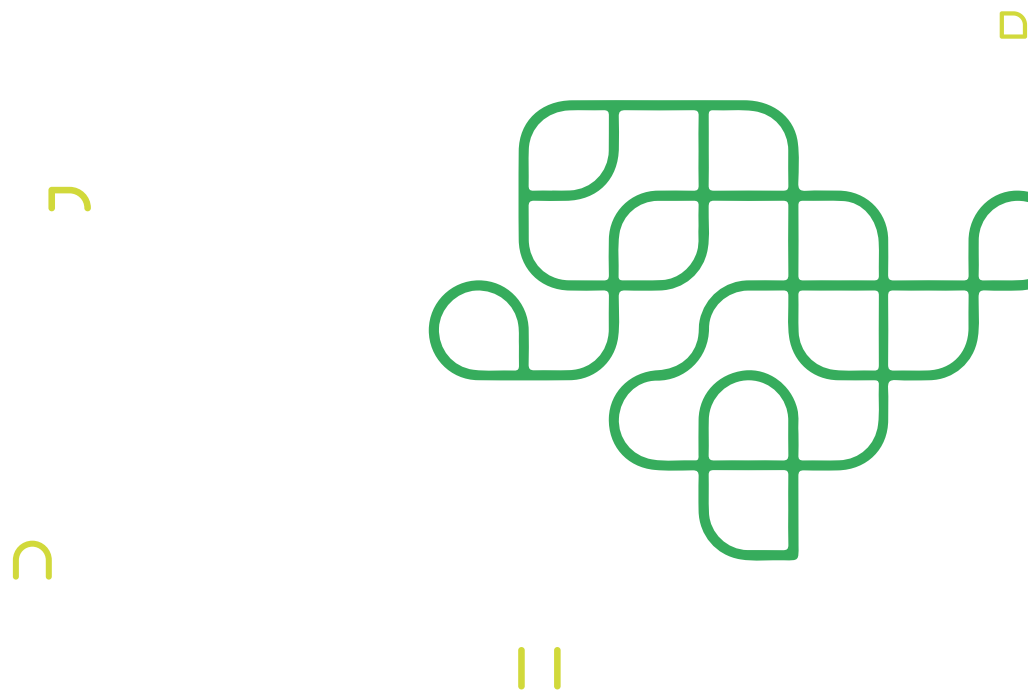
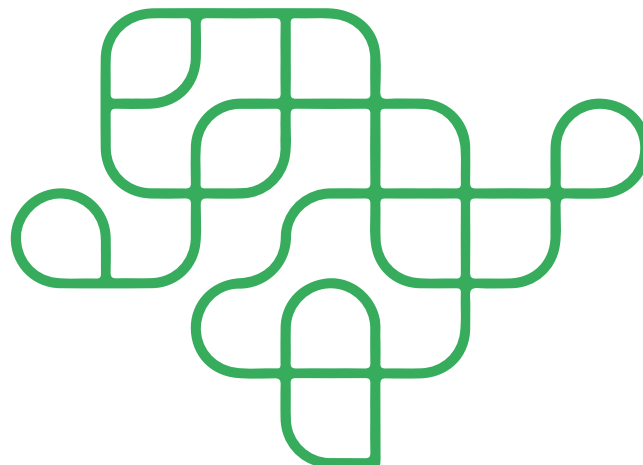
Art. 13-A. É vedada a integração de sistemas de IA usados em segurança pública com bases de dados de serviços públicos sensíveis, como saúde, educação, assistência social ou biometria civil, salvo mediante lei específica que regule os critérios de finalidade, proporcionalidade, necessidade, consentimento e controle externo.

REDAÇÃO ATUAL

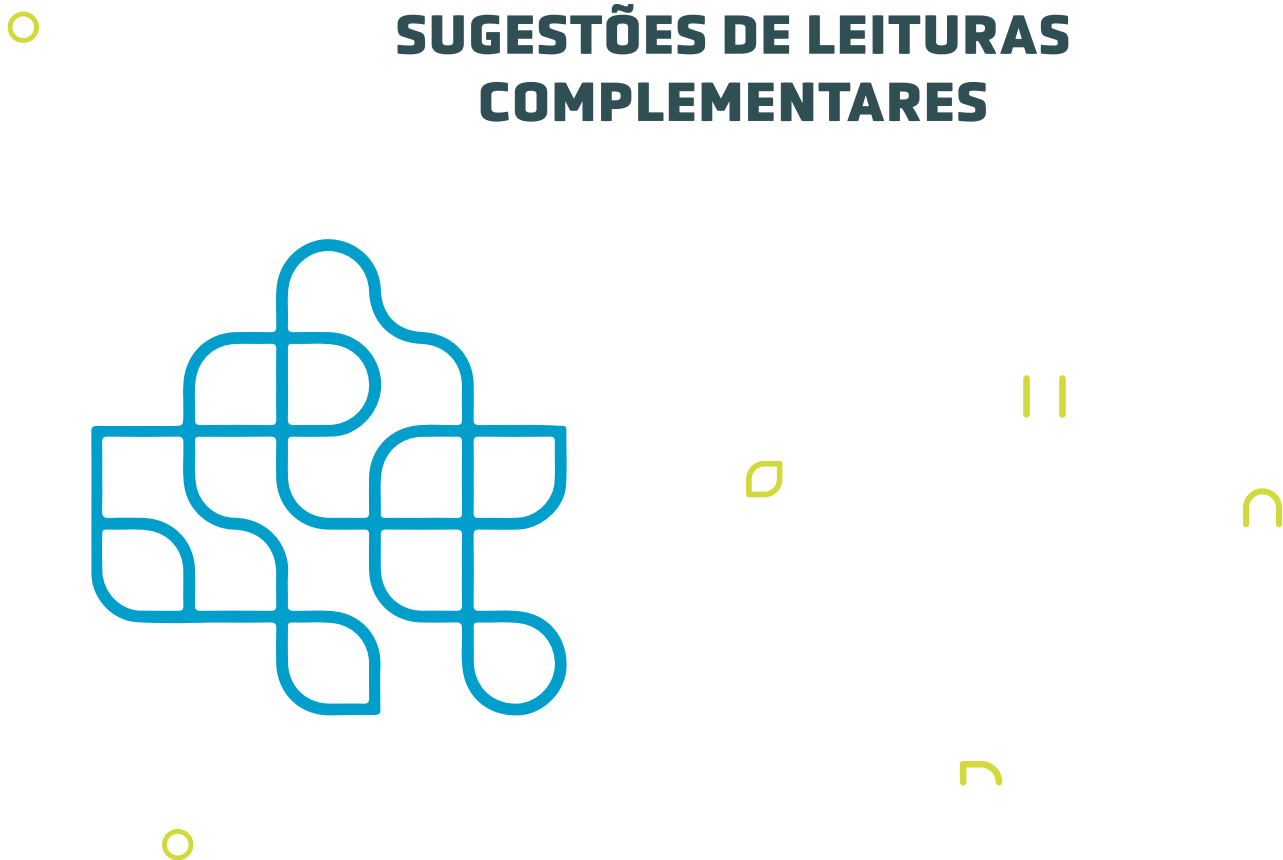
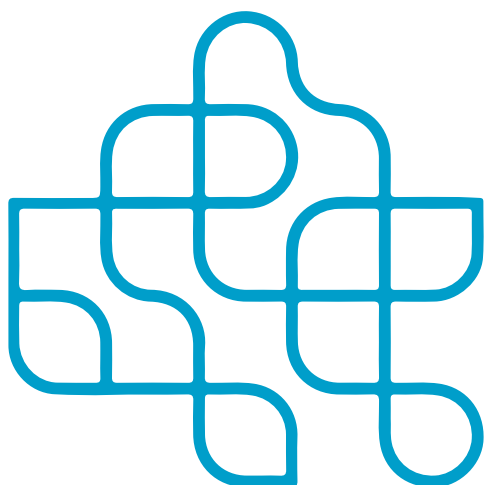
Art. 25 inclusão

PROPOSTA

Art. 25-A. Os sistemas de IA aplicados à segurança pública devem ser precedidos de parecer técnico independente sobre riscos de discriminação algorítmica, emitido por entidade acadêmica, organização da sociedade civil ou perito autônomo com conhecimento técnico reconhecido, previamente credenciado junto ao SIA.



SUGESTÕES DE LEITURAS COMPLEMENTARES



SUGESTÕES DE LEITURAS COMPLEMENTARES

A deep dive into Brazil's data economy: Report on challenges and opportunities

- Produto 2: Recomendações para um marco regulatório de Economia de Dados no Brasil - Novembro de 2024 (principalmente capítulos 1, 2, 5, 6, e 9; e os tópicos “Potenciais Benefícios da Regulamentação”; “Maior confiança para o compartilhamento de dados”).

African Union Data Policy Framework

- 5.3.2.4 DATA JUSTICE
- 5.4 DATA GOVERNANCE
- 5.5. INTERNATIONAL AND REGIONAL GOVERNANCE

BRASIL, Conselho Administrativo de Defesa Econômica. Contribuição ao Projeto de Lei nº 2.338/2023. Brasília/DF. Jan, 2024.

Disponível em https://cdn.cade.gov.br/Portal/assuntos/noticias/2024/Contribui%C3%A7%C3%A3o%20CADE%20PL%202338_final.pdf.

Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPd)

- Seção V Do Comitê de Especialistas e Cientistas de Inteligência Artificial observa as competências e objetivos dispostos no decreto que estrutura o CNPD, em especial, os art.1º e 14.

Constituição Federal

- Art. 170
- Art.219

Data Act

- Capítulo VIII sobre interoperabilidade (em específico parágrafo 90 sobre interoperabilidade e padrões utilizados).

Data Governance Act

- Página da Comissão Europeia “[Data Governance Act explained](#)”.
- Menções a “data spaces” e seus princípios (‘FAIR data principles’).

Declaração de Líderes dos BRICS sobre governança global da Inteligência Artificial

- Parágrafo “A Soberania Digital e o Direito ao Desenvolvimento são Fundamentais para a Governança Global da IA”
- Parágrafo “Vieses Discriminatórios Devem Ser Mitigados”.
- Parágrafo “A Governança de Dados é Chave para uma Governança Inclusiva da IA”.

Declaração de São Luís de grupos de engajamento do G20

- Parágrafo 3 sobre abordagem de justiça de dados e evitar tipos de discriminação
- Parágrafo 4 sobre sustentabilidade
- Parágrafo 5 sobre interoperabilidade
- Parágrafo 13 sobre dados abertos e criação de “data spaces”
- Parágrafo 14 sobre transparência e accountability

Declaração Multissetorial do NetMundial+10

- (Tópico 2) Princípios para Governança da Internet e Processos de Políticas Digitais
- (Tópico 3) Aplicar a abordagem multissetorial e melhorar os processos multilaterais

Estratégia de Dados da ONU

- Glossário - definição de “data governance”

EU AI Act

- Article 10: Data and Data Governance
- Article 67: Advisory Forum
- Article 68: Scientific Panel of Independent Experts

G20 Compendium on Data Access and Sharing Across the Public Sector and with the Private Sector for Public Interest

- Capítulo 2 - Data access and sharing in the public sector (menção ao reuso de dados)

Lei Geral de Proteção de Dados

- Capítulo I, art.6 (dos princípios para o tratamento de dados pessoais);
- Capítulo IV, Seção I, art.25 (sobre interoperabilidade de dados);
- Capítulo IX, Seção II, art.58 (Sobre o Conselho Nacional de Proteção de Dados).

Minuta da Política de Governança e Compartilhamento de Dados

- Art 2º, II - define “governança de dados”
- Art 3º, V - interoperabilidade e compartilhamento de dados observada legislação aplicável

OLIVEIRA, Maria. GOMES, Pollyany. Inteligência artificial generativa e a desinformação no Brasil.

(2024). Seminário Internacional De Informação, Tecnologia E Inovação, 6, e155. <https://observinter.al.org.br/index.php/siti/article/view/155>

Órgão Consultivo de Alto Nível sobre Inteligência Artificial da ONU

- TERMOS DE REFERÊNCIA: (par. 3, sobre engajamento multissetorial)
- GOVERNING AI FOR HUMANITY (relatório do Órgão): Introdução, I. (da composição e competência); Introdução, II. (das consultas)

PACHECO, Denis. Inteligências artificiais entram em campo contra e a favor da desinformação.

Jornal USP. São Paulo/SP. Nov, 2023. Disponível em <https://jornal.usp.br/atualidades/inteligencias-artificiais-entram-em-campo-contr-a-a-favor-da-desinformacao/>

Pacto Global Digital da ONU

- Princípios
 - 8(a) sobre participação coletiva de stakeholders e conectividade (close all digital divides)
 - 8(b) sobre desenvolvimento (development-oriented)
 - 8(c) sobre ser ancorado nos Direitos Humanos
 - 8(d) sobre igualdade de gênero
 - 8(e) sobre sustentabilidade ambiental
 - 8(h) sobre interoperabilidade
 - 8(k) sobre cooperação multissetorial (multistakeholder)
- Objetivo 4 sobre governança de dados
 - parágrafo 37 sobre necessidade de uma governança interoperável para avançar desenvolvimento e proteger Direitos Humanos
 - parágrafo 39(b) sobre fortalecer apoio aos países para desenvolverem abordagens nacionais de governança de dados
 - parágrafo 39(d) sobre ciclo de dados e fins legítimos
 - parágrafo 41 sobre padrões comuns e interoperabilidade voltados para desenvolvimento e com envolvimento de todos os stakeholders

parágrafo 42(a) sobre realização de auditorias para evitar vieses e mitigar abusos

parágrafo 42(c) sobre reuso de dados para o bem público

parágrafo 48 sobre interoperabilidade e cooperação nos níveis nacional, regional, e internacional

- Objetivo 5 sobre governança da inteligência artificial
 - parágrafo 53 sobre governar IA para o interesse público
 - parágrafo 55(b) sobre interoperabilidade de abordagens de governança de IA
 - parágrafo 56(a) de proposta de criação do Painel Científico
 - parágrafo 58 sobre padronização e interoperabilidade de acordo com os Direitos Humanos

Painel Científico da ONU sobre IA

- 1. (da composição do Painel)
- 1. a) (das competências)

Plano Brasileiro de Inteligência Artificial (PBIA)

- Ação 27: Nuvem Soberana;
- Ação 28: Catalogação, Governança e Estratégia de Uso de Dados;
- Ação 29: Integração e Reúso Estratégico de Dados do Eixo 3 – IA para Melhoria dos Serviços Públicos.

Porque o G20 precisa do Data20

- Abordagem de “justiça de dados”, com destaque para o seguinte parágrafo:
“De acordo com as prioridades do Brasil, deve ser explorada a relação entre justiça de dados e transformação digital inclusiva: i) enfatizando a natureza focada de cidadania do conceito, considerando a atual divisão digital que compromete as epistemologias do Sul Global para um planeta igualitário e sustentável; ii) evitando discriminações, trabalho precário e um impacto ambiental desequilibrado que estão ampliando as assimetrias históricas de poder e tornando ainda mais periférica a maioria global do mundo (Global Majority of the World); c) governança de dados é o elemento fundacional para se discutir IA, já que tais tecnologias e o poder computacional em questão não se dá no vácuo e sim alimentado por esses bits de informação.”

Recomendações sobre Acesso e Compartilhamento de Dados da OCDE

- Definição de “data value cycle” (item II)

Regulamento de Execução 2025/454 da UE

- Artigo 6.o: Secretariado
- Artigo 9.o: Remuneração

Social data governance: Towards a definition and model

- Definição de “social data governance”:

“By designating “social” as a prefix for “data governance,” the proposed term entails threefold meanings when addressing data governance. First, it denotes a model or framework that encompasses the quantified calculation, fully or partially, through which information about human behaviors in social contexts is collected, shared, manipulated, interpreted, and represented through (digital) technologies. Second, such a model or framework guides, monitors, provokes, biases, controls, and constrains social behavior (van Dijck, 2014) for the specific purpose of sociopolitical control. Third, the model or framework is constituted and framed, but not necessarily decided, by multifaceted societal elements, such as the political, social, economic, and technological apparatuses and arrangements (Micheli et al., 2020). By highlighting the social dynamics of both data and governance, we seek to avoid the organization-centric pitfalls as far as possible. Our emphasis on such dynamics prioritizes the external macro-level social, political, and economic factors that shape data and governance arrangements.”

T20 Brasil: Task Force 5 Statement

- Abordagem de justiça de dados: Introduction to the Task Force’s mission and priorities
- Recomendação 3 de criação do Data20 (D20), com destaque para o trecho:

“[...] foster a convergent position towards a set of interoperable policy instruments to promote transnational data solidarity, including methods for evaluating and leveraging the public value of data as a common good, aimed at reducing information and power asymmetry. Debating cross-cutting issues on data governance can influence more transparent and fair AI systems and also be diverse in terms of language [...] Additionally, the D20 could enable the development of regulatory parity based on human rights and data justice.”

