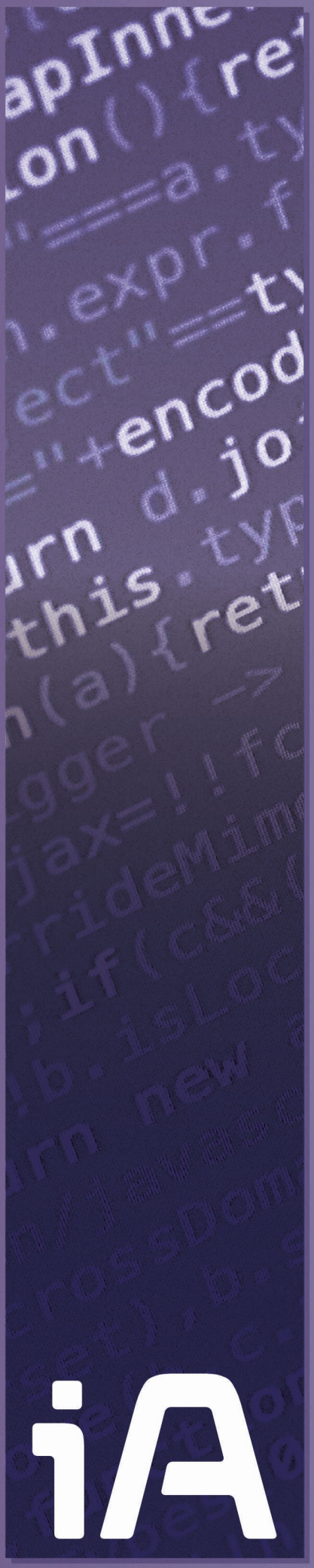

PROJETO DE LEI Nº2338/2023

NOTA TÉCNICA

COALIZÃO DIREITOS NA REDE

AGOSTO, 2023

PROJETO DE LEI Nº2338/2023

NOTA TÉCNICA

COALIZÃO DIREITOS NA REDE

AUTORIA

Laboratório de Políticas Públicas e Internet - LAPIN

Cynthia Picolo Gonzaga de Azevedo

Gabriela Buarque

José Renato Laranjeira de Pereira

REVISÃO

Me Representa

Ladyane Souza

Maria Paula Russo Riva

ELABORADO PARA E COM O APOIO DE

Coalizão Direitos na Rede

LAPIN
LABORATÓRIO DE POLÍTICAS PÚBLICAS E INTERNET

#MEREPRESENTA

Sumário

1 CONTEXTO

Por que regular?

O avanço acelerado no desenvolvimento e uso de sistemas de inteligência artificial (IA) é uma tendência global na qual o Brasil também se insere, que reconfigura a lógica e o funcionamento das sociedades. Otimização na gestão de serviços públicos, automação de processos de negócios, análise e compilação agilizada de dados em pesquisas, avançados diagnósticos de saúde, até a recomendação de músicas na plataforma de streaming, são alguns exemplos de atividades hoje propiciadas ou favorecidas pelo uso da IA. Essa tecnologia já vem sendo implementada amplamente em diversas áreas, como nos setores produtivos, científicos, educacionais, governo e academia, revolucionando a forma que coletivos, organizações e instituições se organizam.

Os benefícios trazidos por esta tecnologia globalmente são, portanto, inegáveis. É também inegável que essa revolução gera impactos, não necessariamente positivos, que se estendem além das fronteiras. No campo ambiental, por exemplo, estudos revelaram que a emissão de dióxido de carbono durante o ciclo de treinamento de grandes modelos de IA corresponde a quase cinco vezes as emissões de vida útil de um carro médio[1].

Outro notável exemplo, em ampla discussão atualmente, é o uso de reconhecimento facial que, por afetar principalmente populações e especialmente grupos historicamente marginalizados, reproduz discriminações e aumenta desigualdades sociais. Em 2018, as pesquisadoras Joy Buolamwini e Timnit Gebru demonstraram que algumas tecnologias de reconhecimento facial produzidas pela IBM, Microsoft e Face++ performavam diferente em relação aos diversos grupos sociais.

Elas identificaram que a taxa de acerto dessas tecnologias era maior para homens brancos e menor para pessoas negras e do gênero feminino[2]. No Brasil, em 2021, além das mais de 800.000 pessoas indígenas, 43% dos brasileiros se auto-declararam como brancos, 47% como pardos e 9,1% como pretos[3], de modo que o uso dessa tecnologia

1 HAO, Karen. **Training a single AI model can emit as much carbon as five cars in their lifetimes. Deep learning has a terrible carbon footprint.** MIT Technology Review. Disponível em: https://www.technologyreview.com/2019/06/06/239031/training-a-single-ai-model-can-emit-as-much-carbon-as-five-cars-in-their-lifetimes/. Acesso em: 03 jul. 2023.

2 BUOLAMWINI, Joy; GEBRU, Timnit. **Gender Shades: Intersectional Accuracy Disparities in Commencial Gender Classification.** 2018. Proceedings of Machine Learning Research, Nova York, v. 8, p. 1-15. Disponível em: http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf. Acesso em: 03 jul. 2023.

3 INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA - IBGE. **Conheça o Brasil.** Disponível em: https://educa.ibge.gov.br/jovens/conheca-o-brasil/populacao/18319-cor-ou-raca.html. Acesso em: 03 jul. 2023.

se torna particularmente problemático. No contexto da segurança pública brasileira já há diversos relatos de prisões injustas por erro do reconhecimento facial[4], além de casos de discriminação em modelos de concessão de crédito[5].

Existe, ainda, outro aspecto que merece atenção: o descompasso entre o rápido desenvolvimento de sistemas cada vez mais avançados, como as IAs generativas, e a capacidade de resposta regulatória. ChatGPT, Bard, Bing e DALLE 2, são alguns exemplos desse tipo de tecnologia, que é capaz de produzir textos, gerar imagens, músicas e conteúdos inéditos. No entanto, podem igualmente se tornar facilitadoras da disseminação de desinformação, reprodutoras de vieses discriminatórios e incentivadoras na redução da autonomia e do pensamento crítico humano[6].

Essas situações ilustram o porquê, para além das oportunidades trazidas pela IA, é urgente refletir e enfrentar os inerentes desafios por ela trazidos, que não se limitam aos ambientais, éticos e sociais. Identificar os benefícios, mapear riscos de forma constante, procurar formas de mitigá-los, promover a responsabilização e garantir o exercício de direitos é o que norteará o avanço tecnológico de maneira sustentável, com sistemas voltados aos problemas de nossa realidade com segurança jurídica, maior robustez nos negócios e valor reputacional.

Nesse contexto, a regulação é mecanismo fundamental para se evitar a perpetuação de discriminações estruturais que são reproduzidas na sociedade. Isso demanda uma responsabilidade ativa que concretize transparência e diversidade, desde a concepção e o design de sistemas de inteligência artificial, sob pena de se chancelar a perpetuação e acirramento de discriminações estruturais e epistêmicas, bem como perspectivas racistas e coloniais.

Regular o uso e desenvolvimento da inteligência artificial é, portanto, proporcionar caminhos para seu uso responsável, além de permitir que esta tecnologia seja instrumento de fomento ao bem estar social, à inovação, educação, avanço científico e produtividade na administração pública.

---

4 TIRE MEU ROSTO DA SUA MIRA. Disponível em: https://tiremeurostodasuamira.org.br/. Acesso em: 03 jul. 2023.

5 SILVA, Tarcízio. **Racismo algorítmico: inteligência artificial e discriminação nas redes digitais.** Edições Sesc SP, 2022. E-book.

6 HACKER, Philip; ENGEL, Andreas; MAUER, Marco. **Regulating ChatGPT and other Large Generative AI Models.** Working Paper, 2023. Disponível em: https://www.law.ox.ac.uk/content/event/regulating-chatgpt-and-other-large-generative-ai-models. Acesso em: 03 jul. 2023.

O debate regulatório sobre inteligência artificial no Brasil

No Brasil, debates regulatórios sobre a IA vêm ganhando força desde o ano de 2020, com a propositura do Projeto de Lei nº 21-A, de 2020 (PL 21-A/2020), de autoria do Deputado Eduardo Bismarck e relatoria da Deputada Luísa Canziani[7]. O trâmite do processo legislativo na Câmara dos Deputados, que correu em regime de urgência e sem ampla participação social, findou-se em 29 de setembro de 2021, com apresentação pela relatora e aprovação de substitutivo que manteve caráter predominantemente principiológico do texto.

A proposta que seguiu para o Senado Federal foi alvo de críticas por não promover um arcabouço que permitisse, dentre outros, a proteção efetiva e operacionalização do exercício de direitos, a definição de obrigações e respectivos instrumentos de governança e um arranjo fiscalizatório.

Em um contexto em que nem ao menos uma avaliação de impacto algorítmico foi prevista, o PL n° 21-20/A ainda optou, em seu artigo 6°, inciso VI, por restringir a responsabilidade dos agentes das da IA à esfera subjetiva, levando em conta "a efetiva participação" destes no dano. Neste modelo, a pessoa afetada precisaria comprovar a culpa do agente pela falha do sistema de IA, cujo comportamento é muitas vezes imprevisível e seu funcionamento é extremamente complexo até mesmo para seus desenvolvedores. Assim, o que se propõe é que a vítima que busca reparação por danos sofridos seja responsável pelo ônus da prova.

O PL nº 21-A/2020 também não avançou em buscar eliminar o uso discriminatório e excessivamente perigoso de certas tecnologias.

Diante da repercussão de diversos setores e da sociedade civil sobre estes e outros problemas, em 17 de fevereiro de 2022 foi instalada uma Comissão de Juristas responsável por subsidiar a elaboração de substitutivo sobre inteligência artificial (CJSUBIA), criada pelo Presidente do Senado Federal, Rodrigo Pacheco (PSD-MG)[8].

A CJSBIA, presidida pelo Ministro do Superior Tribunal de Justiça (STJ) Dr. Ricardo Villas Bôas Cueva, com relatoria da Dra. Laura Schertel Ferreira Mendes, contou com 18 (dezoito) juristas em sua composição. Após rodadas de audiência públicas sobre temas caros à regulação da IA, um seminário com especialistas internacionais

7 CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 21/2020.** Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2236340. Acesso em: 03 jul. 2023.

8 SENADO FEDERAL. **Comissão de Juristas Responsável por Subsidiar a Elaboração de Substitutivo sobre Inteligência Artificial no Brasil** - CJSUBIA. Disponível em: https://legis.senado.leg.br/comissoes/comissao?codcol=2504. Acesso em: 03 jul. 2023.

9 SENADO FEDERAL. **Documentos de audiências públicas.** Disponível em: https://legis.senado.leg.br/comissoes/audiencias?codcol=2504. Acesso em: 03 jul. 2023.

e diversas discussões entre os membros[9], a Comissão de Juristas publicou em 06 de dezembro de 2022 um parecer com uma proposta de substitutivo para instruir a apreciação não somente do PL n° 21-A/2020, como também dos PLs n° 5.051/2019 e 872/2021 - ambos sobre marcos éticos, diretrizes e princípios para o desenvolvimento e uso da IA.

O Senador Rodrigo Pacheco converteu a minuta de substitutivo da Comissão no Projeto de Lei nº 2338/2023 em 6 de maio de 2023, tendo o Senador Eduardo Gomes (PL-TO) como relator. O texto proposto reflete a continuidade dos debates, que avançaram a passos largos desde a propositura do PL n° 21-A/2020 na Câmara dos Deputados. Fenômenos globais, como a pandemia da Covid-19, a popularização de aplicações de IA generativa como o ChatGPT, e esforços nacionais e internacionais para compreender os riscos e estruturas de governança para a IA puseram novos desafios que fizeram o debate a se expandir.

O novo PL, portanto, é reflexo de um processo contínuo de discussões sobre IA, e não deve ser encarado a partir de uma ideia de rivalização com as propostas anteriores[10]. O texto avança ao buscar a conciliação entre uma abordagem regulatória baseada em riscos e outra baseada em direitos fundamentais, incluindo propostas de gestão de risco e avaliação de impacto, ampliação de transparência e contestação de sistemas.

Noutro norte, ainda existem pontos que demandam maior amadurecimento e debate, especialmente no que tange ao uso do reconhecimento facial, segurança pública, autoridade competente e riscos excessivos. Ainda que seja uma proposta mais responsável em comparação com as anteriores, dadas as peculiaridades do Brasil e maior alinhamento às discussões internacionais, são bem-vindos maiores amadurecimento e aperfeiçoamento. Assim, faz-se necessário que as discussões acerca da regulação da IA no Brasil sejam continuadas no Congresso Nacional no âmbito do PL nº 2338/2023, de forma participativa, inclusiva e multissetorial.

O objetivo desta Nota Técnica é justamente contribuir com este debate, reforçando e celebrando os avanços do PL nº 2338/2023 bem como sugestões de melhorias.

---

9 SENADO FEDERAL. **Documentos de audiências públicas.** Disponível em: https://legis.senado.leg.br/comissoes/audiencias?codcol=2504. Acesso em: 03 jul. 2023.

10 COALIZÃO DIREITOS NA REDE - CDR. **Carta de apoio ao PL nº 2338/2023.** Disponível em: https://direitosnarede.org.br/2023/06/14/carta-de-apoio-ao-pl-2338-2023/. Acesso em: 03 jul. 2023.

2 FUNDAMENTOS E PRINCÍPIOS DO PL Nº 2338/2023

O **PL nº 2338/2023** estipula, já em seu **artigo 1º**, que a lei estabelece normas gerais de caráter nacional para o desenvolvimento, implementação e uso responsável de sistemas de IA no Brasil. Nesse cenário, ressalta-se como **ponto primeiro positivo** a preocupação com o desenvolvimento de uma IA responsável e protetiva aos direitos fundamentais.

Na sequência, o **artigo 2º** elenca os fundamentos do desenvolvimento, implementação e uso da IA. Avaliando o rol indicado, é pertinente considerar a **inclusão de um inciso que determine a proteção de crianças, adolescentes, idosos, pessoas com deficiência e demais grupos vulneráveis,** em razão da assimetria informacional e cognitiva, bem como de processos históricos de marginalização dessas pessoas.

Impende sublinhar também que a tutela de grupos vulneráveis é fundamento conectado com o direito à isonomia material (artigo 5º, caput, Constituição Federal)[11], além de mandamento constitucional que vem sendo observado em microssistemas normativos e convenções internacionais, tais como o Estatuto da Criança e do Adolescente (ECA), Convenção sobre os Direitos da Criança, Estatuto do Idoso, Estatuto da Pessoa com Deficiência e Convenção sobre os Direitos da Pessoa com Deficiência e seu Protocolo Facultativo - estes últimos sendo tratados internacionais internalizados no Brasil com caráter de emenda constitucional.

Sendo assim, sob uma perspectiva de integração sistemática do ordenamento jurídico, compete aos novos marcos regulatórios observar ao máximo os mandamentos de proteção constitucional desses grupos historicamente marginalizados.

11 Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes (...).

REDAÇÃO ORIGINAL	REDAÇÃO SUGERIDA
Art. 2º O desenvolvimento, a implementação e o uso de sistemas de inteligência artificial no Brasil têm como fundamentos:	Art. 2º O desenvolvimento, a implementação e o uso de sistemas de inteligência artificial no Brasil têm como fundamentos:
I – a centralidade da pessoa humana;	I – a centralidade da pessoa humana;
II – o respeito aos direitos humanos e aos valores democráticos;	II – o respeito aos direitos humanos e aos valores democráticos;
III – o livre desenvolvimento da personalidade;	III – o livre desenvolvimento da personalidade;
IV – a proteção ao meio ambiente e o desenvolvimento sustentável;	IV – a proteção ao meio ambiente e o desenvolvimento sustentável;
V – a igualdade, a não discriminação, a pluralidade e o respeito aos direitos trabalhistas;	V – a igualdade, a não discriminação, a pluralidade e o respeito aos direitos trabalhistas;
VI – o desenvolvimento tecnológico e a inovação;	VI – o desenvolvimento tecnológico e a inovação;
VII – a livre iniciativa, a livre concorrência e a defesa do consumidor;	VII – a livre iniciativa, a livre concorrência e a defesa do consumidor;
VIII – a privacidade, a proteção de dados e a autodeterminação informativa;	VIII – a privacidade, a proteção de dados e a autodeterminação informativa;
IX – a promoção da pesquisa e do desenvolvimento com a finalidade de estimular a inovação nos setores produtivos e no poder público; e	IX – a promoção da pesquisa e do desenvolvimento com a finalidade de estimular a inovação nos setores produtivos e no poder público; e
X – o acesso à informação e à educação, e a conscientização sobre os sistemas de inteligência artificial e suas aplicações.	X – o acesso à informação e à educação, e a conscientização sobre os sistemas de inteligência artificial e suas aplicações; e
	[incluir inciso] - a proteção de crianças, adolescentes, idosos, pessoas com deficiência e demais grupos vulneráveis.

sugestão de redação ~~sugestão de exclusão~~

Passando-se ao **artigo 3º**, que estipula os **princípios** que norteiam o desenvolvimento, implementação e uso da IA, verifica-se que o **inciso III** traz a "participação humana no ciclo da inteligência artificial e supervisão humana efetiva". Urge ressaltar a necessidade de que o inciso considere a expressão completa, como é utilizada inclusive no inciso IX, qual seja, **"ciclo de vida"**.

A mesma necessidade surge no **inciso VI**, que traz a "transparência, explicabilidade, inteligibilidade e auditabilidade", sendo pertinente reformular o inciso para incluir "transparência, explicabilidade, inteligibilidade e auditabilidade ao longo de todo o ciclo de vida de sistemas de inteligência artificial, como meio de garantir o provimento de informações suficientes para prestação de contas e atribuição de responsabilidades aos agentes de inteligência artificial".

Em continuidade, o **inciso IX** define como princípio a "rastreabilidade das decisões durante o ciclo de vida de sistemas de inteligência artificial como meio de prestação de contas e atribuição de responsabilidades a uma pessoa natural ou jurídica". Nesse ponto, sugere-se a **exclusão** deste inciso, eis que gera confusão com os debates

sobre rastreabilidade de comunicações e a temática já se inclui sob o guarda-chuva do inciso VI ("transparência, explicabilidade, inteligibilidade e auditabilidade"), mencionado acima.

Em relação aos princípios, sugere-se, ainda, a **inclusão de inciso** que estipule o **"desenvolvimento e uso ético e responsável da inteligência artificial"**, de modo a reforçar a centralidade no ser humano e os compromissos internacionais assumidos pelo Estado brasileiro quanto a diretrizes éticas e proteção aos direitos humanos[12]. Além disso, cabe recomendar a inclusão de inciso para a **"proteção e promoção da diversidade de expressões e bens artísticos, culturais e históricos, materiais ou imateriais do país"**. A importância disso por sua vez reside na necessidade de se garantir que esses sistemas não perpetuem o apagamento de conhecimentos tradicionais por meio da reprodução de modelos hegemônicos de pensamento, mais presentes em bases de dados de treinamento.

Ademais, recomendamos a **incorporação do princípio da vulnerabilidade** na forma de inciso. Tal recomendação visa promover equilíbrio em uma relação que é substancialmente desproporcional, uma vez que o elo mais poderoso frequentemente possui recursos e informações privilegiadas, enquanto a parte mais frágil do polo muitas vezes não possui conhecimento técnico suficiente para compreender o funcionamento da IA e suas implicações, que podem ser complexas e opacas[13]. Sendo assim, no que concerne a sistemas automatizados de tomada de decisão, o usuário, pessoa física, natural, deve ter sua vulnerabilidade presumida (absoluta). A pessoa jurídica, por sua vez, deve ser aferida no caso concreto[14].

12 ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **193 países adotam o primeiro acordo global sobre a Ética da Inteligência Artificial**. Novembro, 2021. Disponível em: https://brasil.un.org/pt-br/160484-193-pa%C3%ADses-adotam-o-primeiro-acordo-global-sobre-%C3%A9tica-da-intelig%C3%AAncia-artificial. Acesso em: 12 jul. 2023.

13 BRANCO, Carolina. **O Princípio da Vulnerabilidade na regulamentação de Inteligência Artificial**. IP.rec (blog). Publicado em 18 de abril de 2023. Disponível em: https://ip.rec.br/blog/o-principio-da-vulnerabilidade-na-regulamentacao-da-inteligencia-artificial/. Acesso em: 03 ago 2023.

14 INSTITUTO DE PESQUISA EM DIREITO E TECNOLOGIA DO RECIFE - IP.rec. **Contribuição à consulta pública da Comissão de Juristas do Senado responsável por subsidiar a elaboração de substutivo sobre inteligência artificial no Brasil - CJSUBIA**. IP.rec, 2022. Disponível em: https://ip.rec.br/publicacoes/contribuicao-a-consulta-publica-da-comissao-de-juristas-do-senado-responsavel-por-subsidiar-a-elaboracao-de-substitutivo-sobre-inteligencia-artificial-no-brasil-cjsubia/. Acesso em: 03 ago 2023.

REDAÇÃO ORIGINAL	REDAÇÃO SUGERIDA
Art. 3º O desenvolvimento, implementação e uso de sistemas de inteligência artificial observarão a boa-fé e os seguintes princípios:	Art. 3º O desenvolvimento, implementação e uso de sistemas de inteligência artificial observarão a boa-fé e os seguintes princípios:
I – crescimento inclusivo, desenvolvimento sustentável e bem-estar;	I – crescimento inclusivo, desenvolvimento sustentável e bem-estar;
II – autodeterminação e liberdade de decisão e de escolha;	II – autodeterminação e liberdade de decisão e de escolha;
III – participação humana no ciclo da inteligência artificial e supervisão humana efetiva;	III – participação humana no ciclo de vida da inteligência artificial e supervisão humana efetiva;
IV – não discriminação;	IV – não discriminação;
V – justiça, equidade e inclusão;	V – justiça, equidade e inclusão;
VI – transparência, explicabilidade, inteligibilidade e auditabilidade;	VI – transparência, explicabilidade, inteligibilidade e auditabilidade ao longo de todo o ciclo de vida de sistemas de inteligência artificial, como meio de garantir o provimento de informações suficientes para prestação de contas e atribuição de responsabilidades aos agentes de inteligência artificial;
VII – confiabilidade e robustez dos sistemas de inteligência artificial e segurança da informação;	VII – confiabilidade e robustez dos sistemas de inteligência artificial e segurança da informação;
VIII – devido processo legal, contestabilidade e contraditório;	VIII – devido processo legal, contestabilidade e contraditório;
IX – rastreabilidade das decisões durante o ciclo de vida de sistemas de inteligência artificial como meio de prestação de contas e atribuição de responsabilidades a uma pessoa natural ou jurídica;	~~IX – rastreabilidade das decisões durante o ciclo de vida de sistemas de inteligência artificial como meio de prestação de contas e atribuição de responsabilidades a uma pessoa natural ou jurídica;~~
X – prestação de contas, responsabilização e reparação integral de danos;	X – prestação de contas, responsabilização e reparação integral de danos;
XI – prevenção, precaução e mitigação de riscos sistêmicos derivados de usos intencionais ou não intencionais e efeitos não previstos de sistemas de inteligência artificial; e	XI – prevenção, precaução e mitigação de riscos sistêmicos derivados de usos intencionais ou não intencionais e efeitos não previstos de sistemas de inteligência artificial; e
XII – não maleficência e proporcionalidade entre os métodos empregados e as finalidades determinadas e legítimas dos sistemas de inteligência artificial.	XII – não maleficência e proporcionalidade entre os métodos empregados e as finalidades determinadas e legítimas dos sistemas de inteligência artificial;.
	[incluir inciso] - desenvolvimento e uso ético e responsável da inteligência artificial;
	[incluir inciso] - proteção e promoção da diversidade de expressões e bens artísticos, culturais e históricos, materiais ou imateriais do país; e
	[incluir inciso] - reconhecimento da vulnerabilidade da pessoa natural.

sugestão de redação ~~sugestão de exclusão~~

3 DEFINIÇÕES

No que tange às definições trazidas no artigo 4º, há espaço para aprimoramento. Em primeiro lugar, é necessário que seja **incluída** a definição de **sujeito ou grupo afetado**, enquanto **"pessoa física, ou grupo de pessoas, que sejam direta ou indiretamente sujeitos ou impactados pela decisão de um sistema de IA"**. Isso é importante para garantir que haja uma definição mais detalhada do escopo de proteção da lei, inclusive em relação à proteção de direitos difusos.

Essa consideração é relevante porque, principalmente em se tratando de sistemas de IA, não raro seus reflexos se irradiam para toda a coletividade[15]. Inclusive, esse caráter de proteção coletiva por meio do alongamento de direitos individuais a um grupo encontra paralelo, em nosso ordenamento, no **Código de Defesa do Consumidor**, onde se traz a figura do consumidor por equiparação no parágrafo único do artigo 2º ao estabelecer que a coletividade de pessoas, ainda que indetermináveis, se equipara ao consumidor quando intervir nas relações de consumo.

Em segundo lugar, quanto aos chamados agentes de inteligência artificial, propomos que a diferenciação se dê em relação a **desenvolvedores**, **fornecedores** e **aplicadores da tecnologia**, da seguinte forma:

- **Desenvolvedor:** pessoa física ou jurídica responsável pelo desenvolvimento do sistema de inteligência artificial.
    - **Por desenvolvimento**, entende-se a codificação do algoritmo que baseia o sistema de IA, como também o processo de seleção e utilização das bases de dados, além da criação e treinamento do modelo e eventuais modificações dele antes de sua colocação no mercado ou de ser operacionalizado com possibilidade de geração de impacto a terceiros.
- **Fornecedor:** pessoa física ou jurídica, de natureza pública ou privada, responsável pela disponibilização de sistema de IA para que terceiros o operem a título oneroso ou gratuito.
- **Aplicador:** pessoa física ou jurídica responsável pela implementação e operação de um sistema de IA para atingir um determinado objetivo.

Vale ressaltar que **há casos em que essas figuras se confundem e se sobrepõem**, podendo as entidades que desenvolvem, fornecem e aplicam sistemas serem as

15 AQUINO, Ellen L. de C. **Algoritmos e sociedade: as relações e a complexidade do algoritmo computacional como artefato sociotécnico.** Curitiba: Ed. do Autor, 2022, p. 151.

mesmas em alguns casos. A título de exemplo, uma secretaria municipal que desenvolve ela própria um sistema de aprendizagem de máquina para processar dados de pessoas contaminadas com dengue será tanto desenvolvedora quanto aplicadora do sistema. Nesses casos, a responsabilidade seria aferida tomando como base essa concentração de funções.

Fundamental, ainda, garantir que essas diferenciações estejam refletidas ao longo de todo o texto.

Além disso, **é necessário trazer a definição do termo "ciclo de vida"**, que guiará regras relacionadas à transparência de sistemas de IA e a responsabilização de seus agentes ao longo do texto.

Sugerimos uma redação que tome como pressuposto que esse **ciclo compreenda não só o lapso temporal** em que o sistema encontra-se em funcionamento, ou seja, em estágio já desenvolvido. Deve-se enquadrar também os **momentos de concepção e desenvolvimento do sistema**, de modo a garantir que eventuais violações desta lei nesses momentos, como no caso de não documentação de determinadas decisões, estejam devidamente protegidas. Por isso, sugerimos a seguinte redação:

ciclo de vida: série de fases que engloba desde a concepção, planejamento, desenvolvimento, treinamento, testagem, fornecimento, aplicação e eventuais modificações e adaptações de um sistema de inteligência artificial até a descontinuação de sua aplicação ou o descarte.

REDAÇÃO ORIGINAL	REDAÇÃO SUGERIDA
Art. 4º. Para as finalidades desta Lei, adotam-se as seguintes definições:	Art. 4º. Para as finalidades desta Lei, adotam-se as seguintes definições:
I – **sistema de inteligência artificial:** sistema computacional, com graus diferentes de autonomia, desenhado para inferir como atingir um dado conjunto de objetivos, utilizando abordagens baseadas em aprendizagem de máquina e/ou lógica e representação do conhecimento, por meio de dados de entrada provenientes de máquinas ou humanos, com o objetivo de produzir previsões, recomendações ou decisões que possam influenciar o ambiente virtual ou real.	I – **sistema de inteligência artificial:** sistema computacional, com graus diferentes de autonomia, desenhado para inferir como atingir um dado conjunto de objetivos, utilizando abordagens baseadas em aprendizagem de máquina e/ou lógica e representação do conhecimento, por meio de dados de entrada provenientes de máquinas ou humanos, com o objetivo de produzir previsões, recomendações ou decisões que possam influenciar o ambiente virtual ou real.
II – **fornecedor de sistema de inteligência artificial:** pessoa natural ou jurídica, de natureza pública ou privada, que desenvolva um sistema de inteligência artificial, diretamente ou por encomenda, com vistas à sua colocação no mercado ou à sua aplicação em serviço por ela fornecido, sob seu próprio nome ou marca, a título oneroso ou gratuito;	II – ~~no mercado ou à sua aplicação em serviço por ela fornecido, sob seu próprio nome ou marca, a título oneroso ou gratuito;~~ responsável pela disponibilização de sistema de inteligência artificial para que terceiros o operem a título oneroso ou gratuito.
III – **operador de sistema de inteligência artificial:** pessoa natural ou jurídica, de natureza pública ou privada, que empregue ou utilize, em seu nome ou benefício, sistema de inteligência artificial, salvo se	III – ~~**operador de sistema de inteligência artificial:** pessoa natural ou jurídica, de natureza pública ou privada, que empregue ou utilize, em seu nome ou benefício, sistema de inteligência artificial, salvo se~~

sugestão de redação ~~sugestão de exclusão~~

REDAÇÃO ORIGINAL	REDAÇÃO SUGERIDA
o referido sistema for utilizado no âmbito de uma atividade pessoal de caráter não profissional.	~~o referido sistema for utilizado no âmbito de uma atividade pessoal de caráter não profissional.~~
	aplicador de sistema de inteligência artificial: pessoa física ou jurídica responsável pela implementação e operação de um sistema de inteligência artificial para atingir um determinado objetivo.
IV – **agentes de inteligência artificial:** fornecedores e operadores de sistemas de inteligência artificial.	IV – **agentes de inteligência artificial:** fornecedores e operadores de sistemas de inteligência artificial.
V – **autoridade competente:** órgão ou entidade da Administração Pública Federal responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional;	V – **autoridade competente:** órgão ou entidade da Administração Pública Federal responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional;
VI – **discriminação:** qualquer distinção, exclusão, restrição ou preferência, em qualquer área da vida pública ou privada, cujo propósito ou efeito seja anular ou restringir o reconhecimento, gozo ou exercício, em condições de igualdade, de um ou mais direitos ou liberdades previstos no ordenamento jurídico, em razão de características pessoais como origem geográfica, raça, cor ou etnia, gênero, orientação sexual, classe socioeconômica, idade, deficiência, religião ou opiniões políticas.	VI – **discriminação:** qualquer distinção, exclusão, restrição ou preferência, em qualquer área da vida pública ou privada, cujo propósito ou efeito seja anular ou restringir o reconhecimento, gozo ou exercício, em condições de igualdade, de um ou mais direitos ou liberdades previstos no ordenamento jurídico, em razão de características pessoais como origem geográfica, raça, cor ou etnia, gênero, orientação sexual, classe socioeconômica, idade, deficiência, religião ou opiniões políticas.
VII – **discriminação indireta:** discriminação que ocorre quando normativa, prática ou critério aparentemente neutro tem a capacidade de acarretar desvantagem para pessoas pertencentes a grupo específico, ou as coloquem em desvantagem, a menos que essa normativa, prática ou critério tenha algum objetivo ou justificativa razoável e legítima à luz do direito à igualdade e dos demais direitos fundamentais;	VII – **discriminação indireta:** discriminação que ocorre quando normativa, prática ou critério aparentemente neutro tem a capacidade de acarretar desvantagem para pessoas pertencentes a grupo específico, ou as coloquem em desvantagem, a menos que essa normativa, prática ou critério tenha algum objetivo ou justificativa razoável e legítima à luz do direito à igualdade e dos demais direitos fundamentais;
VIII – **mineração de textos e dados:** processo de extração e análise de grandes quantidades de dados ou de trechos parciais ou integrais de conteúdo textual, a partir dos quais são extraídos padrões e correlações que gerarão informações relevantes para o desenvolvimento ou utilização de sistemas de inteligência artificial.	VIII – **mineração de textos e dados:** processo de extração e análise de grandes quantidades de dados ou de trechos parciais ou integrais de conteúdo textual, a partir dos quais são extraídos padrões e correlações que gerarão informações relevantes para o desenvolvimento ou utilização de sistemas de inteligência artificial.
	[incluir inciso] - sujeito ou grupo afetado: pessoa física, ou grupo de pessoas, que sejam direta ou indiretamente sujeitos ou impactados pela decisão de um sistema de inteligência artificial;
	[incluir inciso] - ciclo de vida: série de fases que engloba desde a concepção, planejamento, desenvolvimento, treinamento, testagem, fornecimento, aplicação e eventuais modificações e adaptações de um sistema de inteligência artificial até a descontinuação de sua aplicação ou o descarte.

sugestão de redação ~~sugestão de exclusão~~

4 DIREITOS

O **artigo 5º** traz um rol de direitos das pessoas afetadas por sistemas de inteligência artificial. Inicialmente, impende salientar que **o rol deve ser compreendido como meramente exemplificativo**, de modo que outros direitos possam ser atribuídos e interpretados, a depender do contexto e da regulação específica do setor.

Nesse ponto, o **inciso I** trouxe o "direito à informação prévia quanto às suas interações com sistemas de inteligência artificial". Sugere-se a reformulação da redação do inciso, para constar o "direito à informação prévia de estar em interação com um sistema de inteligência artificial", tendo em vista que nem sempre é fácil identificar se está interagindo com um ser humano ou com uma IA. Recentemente, inclusive, um engenheiro disse ao público que uma IA teria adquirido consciência[16], porque teria exposto reflexões filosóficas.

Com esse mesmo objetivo, sugere-se a **inclusão de incisos** que estabeleçam o "direito ao provimento de informações breves e de fácil compreensão sobre potenciais riscos e danos aos quais a pessoa pode estar sujeita a partir da interação com o sistema", como também o "direito a informações suficientes, proporcionais e adequadas a respeito do sistema de inteligência artificial, de modo a garantir a compreensão do funcionamento do sistema e de suas decisões, previsões, bem como a contestação de qualquer ação tomada pelo sistema, com ou sem intervenção humana, que possa violar os interesses da pessoa ou direitos individuais ou coletivos".

No **inciso IV**, também sugere-se a **inclusão da expressão "revisão"**, de modo que a redação seja formulada para o "direito à determinação, à revisão e à participação humana em decisões de sistemas de inteligência artificial, levando-se em conta o contexto e o estado da arte do desenvolvimento tecnológico". A inclusão é relevante para assegurar a autonomia humana na condução dos sistemas de IA e também dialogar com o artigo 20 da Lei Geral de Proteção de Dados Pessoais (LGPD).

16 LANDIM, Wilkerson. Engenheiro do Google é afastado por acreditar que IA se tornou consciente. Mundo Conectado. Disponível em: https://mundoconectado.com.br/noticias/v/26069/engenheiro-do-google-e-afastado-por-acreditar-que-ia-se-tornou-consciente. Acesso em: 3 jul. 2023.

REDAÇÃO ORIGINAL	REDAÇÃO SUGERIDA
Art. 5º Pessoas afetadas por sistemas de inteligência artificial têm os seguintes direitos, a serem exercidos na forma e nas condições descritas neste Capítulo:	Art. 5º Pessoas afetadas por sistemas de inteligência artificial têm os seguintes direitos, a serem exercidos na forma e nas condições descritas neste Capítulo:
I – direito à informação prévia quanto às suas interações com sistemas de inteligência artificial;	I – direito à informação prévia ~~quanto às suas~~ de estar em interação~~ões~~ com sistemas de inteligência artificial;
II – direito a explicação sobre a decisão, recomendação ou previsão tomada por sistemas de inteligência artificial;	II – direito à explicação sobre a decisão, recomendação ou previsão tomada por sistemas de inteligência artificial;
III – direito de contestar decisões ou previsões de sistemas de inteligência artificial que produzam efeitos jurídicos ou que impactem de maneira significativa os interesses do afetado;	III – direito de contestar decisões ou previsões de sistemas de inteligência artificial que produzam efeitos jurídicos ou que impactem de maneira significativa os interesses do afetado;
IV – direito à determinação e à participação humana em decisões de sistemas de inteligência artificial, levando-se em conta o contexto e o estado da arte do desenvolvimento tecnológico;	IV – direito à determinação, à revisão e à participação humana em decisões de sistemas de inteligência artificial, levando-se em conta o contexto e o estado da arte do desenvolvimento tecnológico;
V – direito à não-discriminação e à correção de vieses discriminatórios diretos, indiretos, ilegais ou abusivos; e	V – direito à não-discriminação e à correção de vieses discriminatórios diretos, indiretos, ilegais ou abusivos; e
VI – o direito à privacidade e à proteção de dados pessoais, nos termos da legislação pertinente.	VI – o direito à privacidade e à proteção de dados pessoais, nos termos da legislação pertinente.
	[incluir inciso] - direito ao provimento de informações breves e de fácil compreensão sobre potenciais riscos e danos aos quais a pessoa pode estar sujeita a partir da interação com o sistema;
	[incluir inciso] - direito a informações suficientes, proporcionais e adequadas a respeito do sistema de inteligência artificial, de modo a garantir a compreensão do funcionamento do sistema e de suas decisões, previsões, bem como a contestação de qualquer ação tomada pelo sistema, com ou sem intervenção humana, que possa violar os interesses da pessoa ou direitos individuais ou coletivos
Parágrafo único. Os agentes de inteligência artificial informarão, de forma clara e facilmente acessível, os procedimentos necessários para o exercício desses direitos.	Parágrafo único. Os agentes de inteligência artificial informarão, de forma clara e facilmente acessível, os procedimentos necessários para o exercício desses direitos.

sugestão de redação ~~sugestão de exclusão~~

5 TRANSPARÊNCIA

I. Por que transparência é importante e factível?

A seção anterior já introduziu alguns aspectos sobre direitos relativos à transparência. No entanto, cabe aqui uma reflexão mais aprofundada.

Um ponto central na discussão a respeito da regulação de sistemas de IA tem sido a sua **opacidade**, o que tem levado muitas pessoas envolvidas em pesquisas sobre esse tema a considerar essas tecnologias como **"caixas pretas"**[17].

Isso se dá principalmente porque vários sistemas se utilizam de quantidades massivas de dados para identificar padrões que servirão de base para a automação de suas operações, além de suas operações envolverem complexos caminhos para análise dessas informações, como é o que ocorre com **sistemas de aprendizagem profunda** (deep learning).

Essa característica, que está presente em sistemas de geração de imagens e textos como por exemplo o **ChatGPT** e **Stable Diffusion**, mas também sistemas de **personalização de conteúdo** em redes sociais ou de **reconhecimento facial**, torna difícil compreender de que forma um sistema chegou a determinado resultado. Afinal, são tantos dados analisados em tamanha velocidade e em procedimentos tão complexos que uma pessoa é incapaz de compreender de que forma um específico resultado foi emitido pela tecnologia. Além disso, a cada novo funcionamento do sistema, ele se transforma e, no jargão computacional, aprende novas informações a partir dos novos dados que acessa. Dessa forma, pode-se considerar que **o sistema está em constante mutação.**

Ocorre que essas narrativas de caixas pretas e opacidade, geralmente ligadas à frequente falta de responsabilização por resultados injustos ou ilegais incorridos por diferentes modelos de inteligência artificial[18], na realidade têm sido vistas por muitos como uma **desculpa** conveniente para guardar segredos comerciais de quem os desenvolve[19]. Ao jogar com a ideia de complexidade de algoritmos,

17 CARABANTES, Manuel. Black-box artificial intelligence: an epistemological and critical analysis. AI & Society 35, 309–317 (2020). Disponível em: https://link.springer.com/article/10.1007/s00146-019-00888-w#citeas; ZEDNIK, Carlos; BOELSEN, Hannes (ed). Overcoming Opacity in Machine Learning. Annual Convention of the Society for the Study of Artificial Intelligence and Simulation of Behaviour, 2021. Disponível em: http://explanations.ai/symposium/AISB21_Opacity_Proceedings.pdf#page=20. Acesso em: 05 jul. 2023.

18 MOHSENI, Sin; ZAREI, Niloofar; RAGAN, Eric D. A Multidisciplinary Survey and Framework for Design and Evaluation of Explainable AI Systems. ACM Trans. Interact. Intell. Syst. 11, 3–4, Article 24, 2021. Disponível em: https://doi.org/10.1145/3387166. Acesso em: 05 jul. 2023.

19 PASQUALE, Frank. The Black Box Society: the secret algorithms that control mo- ney and information. Cambridge, Massachusetts: Harvard University Press, 2015.

os desenvolvedores dessas tecnologias sustentam uma **narrativa que lhes tira a responsabilidade de ter de prestar contas e de se responsabilizar por efeitos negativos de seus produtos justamente em virtude do fator "caixa preta" dessas tecnologias[20].**

Por isso é que muito se tem discutido sobre o desenvolvimento de técnicas para compreender esses sistemas. Por um lado, a realização de **auditorias** — sejam elas de governança, dos modelos de IA em si (em momento pós treinamento dos dados, mas antes de sua utilização) ou de aplicações específicas deles — se torna um método factível e **indispensável** para apoiar na identificação de falhas e riscos dessas tecnologias[21]. Por outro, o desenvolvimento de métodos técnicos de interpretabilidade e explicabilidade que busquem criar ou aprimorar o provimento de informação a respeito do funcionamento dessas tecnologias.

Esses métodos têm demonstrado que sim, **é possível avaliar a legalidade de sistemas de inteligência artificial ainda que não se consiga identificar exatamente como chegaram a determinado resultado.** Eles permitem, por exemplo, que, por meio de análises das bases de dados utilizadas para treinar esses sistemas, se descubram vieses discriminatórios que levem a resultados que discriminam contra pessoas negras por falta de representatividade dessas populações. Ou que, por meio do desenvolvimento de bots, se identifique vieses de gênero em algoritmos de plataformas de música analisando diretamente suas recomendações de artistas[22].

Com isso, **transparência é um princípio fundamental que deve nortear a avaliação dessas tecnologias, e deve se dar de forma ampla.** Afinal, diferentes informações sobre um sistema de IA interessam a: cientistas que queiram estudar um sistema; organizações da sociedade civil que queiram contestar o uso de determinado algoritmo de avaliação de políticas públicas; uma pessoa idosa que queira entender por que teve um empréstimo negado por um sistema algorítmico; ou a um regulador que queira entender de que forma um chatbot possa estar sendo usado para coletar dados pessoais de forma desproporcional.

Além disso, é fundamental que o texto legal reflita a tendência de que **transparência importa não somente para se compreender o funcionamento técnico de um sistema, mas também outras questões envolvidas em seu desenvolvimento e aplicação.**

---

20 LARANJEIRA DE PEREIRA, José Renato. 2022. Openness doesn't hurt: Enforcing qualified machine learning transparency for data protection through responsive regulation. Dissertação de Mestrado, Faculdade de Direito, Universidade de Brasília, Brasília, DF, p. 183. Disponível em: https://repositorio.unb.br/handle/10482/45316. Acesso em: 05 jul. 2023.

21 MÖKANDER, J. et al. **Auditing large language models: a three-layered approach.** AI Ethics (2023). Disponível em: https://doi.org/10.1007/s43681-023-00289-2. Acesso em: 03 jul. 2023.

22 INTERNETLAB. **Algo_Ritmos.** 2023. Disponível em: https://algoritmos.internetlab.org.br/. Acesso em: 05 jul.2023.

Com isso em mente, tratamos agora em mais detalhes sobre como deve ser uma estrutura abrangente de fornecimento de informações para o PL n° 2338/2023.

II. Recomendações

a) Direito à informação para sujeitos afetados

O caput do **artigo 7º** abre margem para que se restrinja o exercício do direito à informação a casos em que o próprio indivíduo contrata ou utiliza, ele próprio, determinado sistema. Isso porque deixa de fora inúmeros casos nos quais indivíduos são sujeitos, de forma passiva, aos resultados da aplicação desses sistemas, como ocorre com sistemas de reconhecimento facial utilizados em espaços públicos ou na avaliação do perfil de crédito de uma pessoa por um banco.

Em ambos os casos, não é a pessoa que contrata ou utiliza o serviço, mas mesmo assim é diretamente impactada por seu uso. **É válido ao artigo 7º, portanto, menção a casos em que o sujeito é impactado por esses sistemas mesmo quando a contratação ou utilização se dá por terceiros,** de forma similar ao que diz o §2º do mesmo artigo ao referir-se a sistemas biométricos.

Neste sentido, sugere-se que a redação seja reformulada do seguinte modo: "as pessoas afetadas por sistemas de inteligência artificial têm o direito de receber, previamente à contratação ou utilização do sistema, ou, ainda, sempre que interagirem com sistema ou tiverem dados pessoais tratados por ele, informações claras, proporcionais, adequadas e em formato acessível".

Na sequência, os **incisos I a VII do artigo 7º** trazem os **aspectos que devem estar contidos na informação transmitida às pessoas afetadas.** Nesse rol, cabe sugerir a **adição de um inciso** que inclua "qualquer outra informação que seja necessária para o exercício de direitos previstos em lei ou para a reparação de eventuais danos que possam sofrer a partir do funcionamento do sistema". Essa redação possibilita maior abertura para o exercício de direitos fundamentais e para a concretização da reparação integral de danos.

Além disso, é fundamental que toda informação prestada a respeito do sistema ao sujeito afetado seja suficiente para que este compreenda seu funcionamento e suas decisões e previsões. O objetivo dessas informações é que o sujeito tenha **evidência suficiente para identificar potenciais violações de seus direitos pelo sistema.** Portanto, devem ser providas de forma clara, concisa, em linguagem de fácil compreensão, e permitir, especialmente em casos de usos de sistemas de alto risco, mecanismos para requisição de mais informações.

Por fim, é importante que a regulação garanta mecanismos de proteção contra o que se chama de "opacidade por transparência". Trata-se do fornecimento de informações em excesso para que seja impossível a outra pessoa ler tudo que ali contém. Com isso, apesar de, em teoria, muitas vezes esse tipo de ação cumprir com requisitos de fornecimento de informação, ela não cumpre com o objetivo fundamental de provimento de transparência qualificada, já que impede a compreensão efetiva de seu conteúdo.

REDAÇÃO ORIGINAL	REDAÇÃO SUGERIDA
Art. 7º Pessoas afetadas por sistemas de inteligência artificial têm o direito de receber, previamente à contratação ou utilização do sistema de inteligência artificial, informações claras e adequadas quanto aos seguintes aspectos:	Art. 7º Pessoas afetadas por sistemas de inteligência artificial têm o direito de receber, previamente à contratação ou utilização do sistema, **ou, ainda, sempre que interagirem com sistema ou tiverem dados pessoais tratados por ele,** informações claras, adequadas e com **linguagem acessível** quanto aos seguintes aspectos:
I – caráter automatizado da interação e da decisão em processos ou produtos que afetem a pessoa;	I – caráter automatizado da interação e da decisão em processos ou produtos que afetem a pessoa;
II – descrição geral do sistema, tipos de decisões, recomendações ou previsões que se destina a fazer e consequências de sua utilização para a pessoa;	II – descrição geral do sistema, tipos de decisões, recomendações ou previsões que se destina a fazer e consequências de sua utilização para a pessoa;
III – identificação dos operadores do sistema de inteligência artificial e medidas de governança adotadas no desenvolvimento e emprego do sistema pela organização;	III – identificação dos operadores do sistema de inteligência artificial e medidas de governança adotadas no desenvolvimento e emprego do sistema pela organização;
IV – papel do sistema de inteligência artificial e dos humanos envolvidos no processo de tomada de decisão, previsão ou recomendação;	IV – papel do sistema de inteligência artificial e dos humanos envolvidos no processo de tomada de decisão, previsão ou recomendação;
V – categorias de dados pessoais utilizados no contexto do funcionamento do sistema de inteligência artificial;	V – categorias de dados pessoais utilizados no contexto do funcionamento do sistema de inteligência artificial;
VI – medidas de segurança, de não-discriminação e de confiabilidade adotadas, incluindo acurácia, precisão e cobertura; e	VI – medidas de segurança, de não-discriminação e de confiabilidade adotadas, incluindo acurácia, precisão e cobertura; e
VII – outras informações definidas em regulamento.	VII – outras informações definidas em regulamento.
	[incluir inciso] - qualquer outra informação que seja necessária para o exercício de direitos previstos em lei ou para a reparação de eventuais danos que possam sofrer a partir do funcionamento do sistema.

sugestão de redação ~~sugestão de exclusão~~

REDAÇÃO ORIGINAL	REDAÇÃO SUGERIDA
§ 1º Sem prejuízo do fornecimento de informações de maneira completa em meio físico ou digital aberto ao público, a informação referida no inciso I do caput deste artigo será também fornecida, quando couber, com o uso de ícones ou símbolos facilmente reconhecíveis.	§ 1º Sem prejuízo do fornecimento de informações de maneira completa em meio físico ou digital aberto ao público, a informação referida no inciso I do caput deste artigo será também fornecida, quando couber, com o uso de ícones ou símbolos facilmente reconhecíveis.
§ 2º Pessoas expostas a sistemas de reconhecimento de emoções ou a sistemas de categorização biométrica serão informadas sobre a utilização e o funcionamento do sistema no ambiente em que ocorrer a exposição.	~~§ 2º Pessoas expostas a sistemas de reconhecimento de emoções ou a sistemas de categorização biométrica serão informadas sobre a utilização e o funcionamento do sistema no ambiente em que ocorrer a exposição.~~ *** sobre a exclusão do § 2º, ver seção 6 abaixo "Categorização de riscos".**
§ 3º Os sistemas de inteligência artificial que se destinem a grupos vulneráveis, tais como crianças, adolescentes, idosos e pessoas com deficiência, serão desenvolvidos de tal modo que essas pessoas consigam entender o seu funcionamento e seus direitos em face dos agentes de inteligência artificial.	§ 3º Os sistemas de inteligência artificial que se destinem a grupos vulneráveis, tais como crianças, adolescentes, idosos e pessoas com deficiência, serão desenvolvidos de tal modo que essas pessoas consigam entender o seu funcionamento e seus direitos em face dos agentes de inteligência artificial.

sugestão de redação ~~sugestão de exclusão~~

b) Adesão a código de boas práticas e de governança

O artigo 30 também merece reflexões para aprimoramento. Ele abre a possibilidade para que agentes de IA, de maneira individual ou coletiva, estabeleçam **códigos de boas práticas** e de **governança** de modo a se criar uma estrutura organizacional com procedimentos transparentes, mecanismos para exercício de direitos, medidas de segurança e de gestão de riscos. Na sequência, os parágrafos 2° e 3° trazem balizas sobre o que se considerar em ambos os instrumentos.

A voluntária adesão a códigos de boas práticas e governança pode, de acordo com o parágrafo 3°, indicar boa-fé, devendo ser levada em consideração quando da análise em fase sancionadora. No entanto, para que seja considerada uma atenuante na aplicação de sanções administrativas é preciso que haja mais que uma adesão voluntária, visando inclusive combater procedimentos organizacionais pró-forma.

Assim, sugere-se a **inclusão, no parágrafo 3°**, de que a adesão voluntária a código de boas práticas e governança pode ser considerada indicativo de boa-fé se comprovado que o programa atende aos requisitos dispostos naquele capítulo (VII) e que os agentes de IA comprovem que envidaram esforços para a implementação de tais instrumentos de governança.

Recomendamos, portanto, a seguinte redação:

REDAÇÃO ORIGINAL	REDAÇÃO SUGERIDA
Art. 30. Os agentes de inteligência artificial 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 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.	Art. 30. Os agentes de inteligência artificial 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 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.
§ 1º Ao se estabelecerem regras de boas práticas, serão consideradas a finalidade, a probabilidade e a gravidade dos riscos e dos benefícios decorrentes, a exemplo da metodologia disposta no art. 24 desta Lei.	§ 1º Ao se estabelecerem regras de boas práticas, serão consideradas a finalidade, a probabilidade e a gravidade dos riscos e dos benefícios decorrentes, a exemplo da metodologia disposta no art. 24 desta Lei.
§ 2º Os desenvolvedores e operadores de sistemas de inteligência artificial, poderão:	§ 2º Os desenvolvedores e operadores de sistemas de inteligência artificial, poderão:
I – implementar programa de governança que, no mínimo:	I – implementar programa de governança que, no mínimo:
a) demonstre o seu comprometimento em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à não maleficência e proporcionalidade entre os métodos empregados e as finalidades determinadas e legítimas dos sistemas de inteligência artificial;	a) demonstre o seu comprometimento em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à não maleficência e proporcionalidade entre os métodos empregados e as finalidades determinadas e legítimas dos sistemas de inteligência artificial;
b) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como ao seu potencial danoso;	b) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como ao seu potencial danoso;
c) tenha o objetivo de estabelecer relação de confiança com as pessoas afetadas, por meio de atuação transparente e que assegure mecanismos de participação nos termos do art. 24, § 3º, desta Lei;	c) tenha o objetivo de estabelecer relação de confiança com as pessoas afetadas, por meio de atuação transparente e que assegure mecanismos de participação nos termos do art. 24, § 3º, desta Lei;
d) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;	d) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;
e) conte com planos de resposta para reversão dos possíveis resultados prejudiciais do sistema de inteligência artificial; e	e) conte com planos de resposta para reversão dos possíveis resultados prejudiciais do sistema de inteligência artificial; e
f) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas.	f) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas.

sugestão de redação ~~sugestão de exclusão~~

REDAÇÃO ORIGINAL	REDAÇÃO SUGERIDA
§ 3º A adesão voluntária a código de boas práticas e governança pode ser considerada indicativo de boa-fé por parte do agente e será levada em consideração pela autoridade competente para fins de aplicação de sanções administrativas.	§ 3º A adesão voluntária a código de boas práticas e governança pode ser considerada indicativo de boa-fé por parte do agente de inteligência artificial e será levada em consideração pela autoridade competente para fins de aplicação de sanções administrativas se comprovada que a adesão atende aos requisitos dispostos neste Capítulo e que foram envidados esforços para a sua efetiva implementação.
§ 4º A autoridade competente poderá estabelecer procedimento de análise de compatibilidade do código de conduta com a legislação vigente, com vistas à sua aprovação, publicização e atualização periódica.	§ 4º A autoridade competente poderá estabelecer procedimento de análise de compatibilidade do código de conduta com a legislação vigente, com vistas à sua aprovação, publicização e atualização periódica.

sugestão de redação ~~sugestão de exclusão~~

c) Auditorias

Outro aspecto de melhoria do PL é a importância de incluir-se **obrigações ou prerrogativas específicas para realização de auditorias desses sistemas,** aspecto que é mencionado de **forma vaga no artigo 3º, VI**, enquanto princípio, mas que não é aprofundado ao longo do texto.

Isso porque, ainda que haja mecanismos de aumento de transparência ao indivíduo, o PL n° 2338/2023 deve garantir prerrogativas para uma avaliação mais ampla desses sistemas por entidades especializadas. Isso deve se dar de modo a garantir que se cubra aspectos mais gerais de seu funcionamento, de maneira independente das informações curadas pelo próprio agente de IA, mas que seja avaliada pela própria autoridade competente ou por outro ente especializado.

A auditoria no caso da IA pode ser compreendida como um leque de abordagens para revisar sistemas[23]. Essa avaliação pode se dar para os mais variados fins, como **(1)** analisar a governança desses sistemas para verificar, por exemplo, de que forma se dá a revisão humana em seu ciclo de tomada de decisões via uma checagem de documentos internos do aplicador; **(2)** analisar o modelo algorítmico em si, como para buscar vieses racistas em seus dados de treinamento; ou **(3)** analisar os outputs do sistema, de modo a compreender sua precisão. Isso pode ser feito tanto por auditorias especializadas contratadas pelo próprio agente de IA, por um regulador ou por pesquisadores, entidades da sociedade civil ou outra entidade com expertise no tema[24].

23 REINO UNIDO. **Auditing algorithms: the existing landscape, role of regulators and future outlook.** Digital Regulation Cooperation Forum, 2022. Disponível em: https://www.gov.uk/government/publications/findings-from-the-drcf-algorithmic-processing-workstream-spring-2022/auditing-algorithms-the-existing-landscape-role-of-regulators-and-future-outlook#:~:text=Algorithmic%20auditing%20refers%20to%20a,to%20inspecting%20its%20inner%20workings. Acesso em: 05 jul. 2023.

24 MÖKANDER, J. et al. **Auditing large language models: a three-layered approach.** AI Ethics, 2023. Disponível em: https://doi.org/10.1007/s43681-023-00289-2. Acesso em: 05 jul. 2023.

A capacidade de realizar auditorias desses sistemas é fundamental para que se possa **compreender, para além das informações providas pelo próprio agente de IA,** que pode ter seus próprios vieses e interesses na veiculação de informações, **se realmente o sistema está em conformidade com o direito.**

Por isso, **é fundamental que, em primeiro lugar, o poder público tenha autonomia para auditar sistemas de IA independentemente de segredos industriais.** Afinal, se há potencial para violação de direitos fundamentais, deve o Estado atuar para garantir a proteção de indivíduos e grupos, sem estar atrelado a interesses comerciais. De modo a garantir a proteção das informações acessadas, mecanismos de responsabilização, tanto do Estado quanto dos agentes que em nome dele atuem, são cabíveis de serem previstas auditorias. Isso especialmente no que diz respeito à defesa do meio ambiente, do consumidor e para redução das desigualdades, como previsto no artigo 170 da Constituição Federal.

Para além disso, **mecanismos devem ser estabelecidos para que especialistas independentes, ou seja, de fora da estrutura estatal, além de entidades da sociedade civil, também possam realizar auditorias e requisitar informações para defender interesses coletivos.** É o que já propõe, por exemplo, o Digital Services Act (DSA), norma aprovada pela União Europeia que prevê a participação desses atores na investigação de sistemas de IA utilizados por grandes plataformas digitais.

Esses agentes seriam credenciados pelo Estado para atuar em auditorias específicas a serem determinadas pela autoridade competente que determinaria quais seriam as informações a que poderiam ter acesso, e estariam sujeitos a mecanismos de responsabilização similares aos mencionados acima em relação ao poder público.

É fundamental, portanto, que haja previsão dessas competências para auditoria em meio às competências da autoridade no artigo 32.

Esse mecanismo de **governança participativa para a IA**[25] relaciona-se com situações recentes em que pesquisadores independentes foram cruciais para identificar falhas em sistemas algorítmicos. Foi o caso de estudos em sistemas usados em planos de saúde que possuíam vieses raciais[26] em carros autônomos que apresentaram problemas para detectar pedestres negros[27], além do famoso caso da ProPublica, em que pesquisadores e defensores da sociedade civil descobriram que o algoritmo COMPAS, usado para prever a probabilidade de reincidência em liberdade condicional, discriminava detentos afro-americanos[28].

25 KAMINSKY, Margot E. e MALGIERI, Gianclaudio. **Algorithmic Impact Assess- ments under the GDPR: Producing Multi-layered Explanations.** International Data Privacy Law, U of Colorado Law Legal Studies Research Paper n. 19-28, 2020. Disponível em: https://ssrn.com/abstract=3456224. Acesso em 29 jun. 2023.

26 OBERMEYER, Z. e MULLAINTHAN, S. **Dissecting Racial Bias in an Algorithm that Guides Health Decisions for 70M People.** Proceedings of the Conference on Fairness, Accountability, and Transparency [online], 2019. Disponível em: https://dl.acm.org/doi/10.1145/3287560.3287593. Acesso em: 29 jun. 2023.

Outro caso foi o que ocorreu com o Twitter quando usuários identificaram que seus algoritmos responsáveis por cortar imagens para fazer caber no feed da plataforma apresentavam comportamento racista, ao privilegiarem pessoas brancas em detrimento das negras na hora de selecionar essas imagens, e misógino, ao privilegiar o corpo de mulheres a seus rostos. Trata-se de um caso que foi identificado, portanto, não por especialistas, mas pelos próprios usuários da plataforma. Posteriormente, pesquisadoras independentes realizaram suas próprias auditorias comprovando as denúncias feitas por usuários.

Esses casos são representativos do importante papel que pesquisadores independentes podem ter em endereçar os impactos negativos da IA, inclusive de modo a reduzir custos estatais. Recomendamos, portanto, a inclusão dos seguintes dispositivos:

* algumas sugestões aqui propostas também são embasadas na seção 7 - "Autoridade Competente"

REDAÇÃO ORIGINAL	*REDAÇÃO SUGERIDA
Art. 32. O Poder Executivo designará autoridade competente para zelar pela implementação e fiscalização da presente Lei.	Art. 32. O Poder Executivo designará autoridade competente, com autonomia funcional, decisória, administrativa e financeira, para zelar pela implementação e fiscalização da presente Lei.
Parágrafo único. Cabe à autoridade competente:	~~Parágrafo único.~~ § 1º Cabe à autoridade competente:
I – zelar pela proteção a direitos fundamentais e a demais direitos afetados pela utilização de sistemas de inteligência artificial;	I – zelar pela proteção a direitos fundamentais e a demais direitos afetados pela utilização de sistemas de inteligência artificial;
II – promover a elaboração, atualização e implementação da Estratégia Brasileira de Inteligência Artificial junto aos órgãos de competência correlata;	II – promover a elaboração, atualização e implementação da Estratégia Brasileira de Inteligência Artificial junto aos órgãos de competência correlata;
III – promover e elaborar estudos sobre boas práticas no desenvolvimento e utilização de sistemas de inteligência artificial;	III – promover e elaborar estudos sobre boas práticas no desenvolvimento e utilização de sistemas de inteligência artificial;
IV – estimular a adoção de boas práticas, inclusive códigos de conduta, no desenvolvimento e utilização	IV – estimular a adoção de boas práticas, inclusive códigos de conduta, no desenvolvimento e utilização

sugestão de redação ~~sugestão de exclusão~~

27 WILSON, B. et al. **Predictive Inequity in Object Detection.** Arxiv. Disponível em: https://arxiv.org/pdf/1902.11097.pdf. Acesso em: 29 jun. 2023.

28 LARSON, J. et al. **How We Analyzed the COMPAS Recidivism Algorithm.** Pro Publica. 2016. Disponível em: https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm. Acesso em: 29 jun. 2023.

29 BIRHANE, Abeba; PRABHU, Vinay Uday; WHALEY, John. **Auditing Saliency Cropping Algorithms.** Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision (WACV), 2022, pp. 4051-4059. Disponível em: https://openaccess.thecvf.com/content/WACV2022/papers/Birhane_Auditing_Saliency_Cropping_Algorithms_WACV_2022_paper.pdf. Acesso em: 05 jul. 2023.

30 ALÌ, Gabriele Spina; YU, Ronald. **Artificial Intelligence between Transparency and Secrecy: from the EC white paper to the AYA and beyond.** European Journal of Law and Technology. Disponível em: https://ejlt.org/index.php/ejlt/article/view/754. Acesso em: 29 jun. 2023.

REDAÇÃO ORIGINAL	REDAÇÃO SUGERIDA
de sistemas de inteligência artificial;	de sistemas de inteligência artificial;
V – promover ações de cooperação com autoridades de proteção e de fomento ao desenvolvimento e à utilização dos sistemas de inteligência artificial de outros países, de natureza internacional ou transnacional;	V – promover ações de cooperação com autoridades de proteção e de fomento ao desenvolvimento e à utilização dos sistemas de inteligência artificial de outros países, de natureza internacional ou transnacional;
VI – expedir normas para a regulamentação desta Lei, inclusive sobre:	VI – expedir normas para a regulamentação desta Lei, inclusive sobre:
a) procedimentos associados ao exercício dos direitos previstos nesta Lei;	a) procedimentos associados ao exercício dos direitos previstos nesta Lei;
b) procedimentos e requisitos para elaboração da avaliação de impacto algorítmico;	b) procedimentos e requisitos para elaboração da avaliação de impacto algorítmico;
c) forma e requisitos das informações a serem publicizadas sobre a utilização de sistemas de inteligência artificial; e	c) forma e requisitos das informações a serem publicizadas sobre a utilização de sistemas de inteligência artificial; e
d) procedimentos para certificação do desenvolvimento e utilização de sistemas de alto risco.	d) procedimentos para certificação do desenvolvimento e utilização de sistemas de alto risco;
	e) procedimentos para a comunicação de incidentes graves, tais como aqueles que afetem direitos fundamentais.
VII – articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação;	VII – articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação;
VIII – fiscalizar, de modo independente ou em conjunto com outros órgãos públicos competentes, a divulgação das informações previstas nos arts. 7º e 43;	VIII – fiscalizar, de modo independente ou em conjunto com outros órgãos públicos competentes, a divulgação das informações previstas nos arts. 7º e 43;
IX – fiscalizar e aplicar sanções em caso de desenvolvimento ou utilização de sistemas de inteligência artificial realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso;	IX – fiscalizar e aplicar sanções em caso de desenvolvimento ou utilização de sistemas de inteligência artificial realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso;
X – solicitar, a qualquer momento, às entidades do poder público que desenvolvam ou utilizem sistemas de inteligência artificial, informe específico sobre o âmbito, a natureza dos dados e os demais detalhes do tratamento realizado, com a possibilidade de emitir parecer técnico complementar para garantir o cumprimento desta Lei;	X – solicitar, a qualquer momento, às entidades do poder público que desenvolvam ou utilizem sistemas de inteligência artificial, informe específico sobre o âmbito, a natureza dos dados e os demais detalhes do tratamento realizado, com a possibilidade de emitir parecer técnico complementar para garantir o cumprimento desta Lei;
XI – celebrar, a qualquer momento, compromisso com agentes de inteligência artificial 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;	XI – celebrar, a qualquer momento, compromisso com agentes de inteligência artificial 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;

sugestão de redação ~~sugestão de exclusão~~

REDAÇÃO ORIGINAL	REDAÇÃO SUGERIDA
XII – apreciar petições em face do operador de sistema de inteligência artificial após comprovada apresentação de reclamação não solucionada no prazo estabelecido em regulamentação; e	XII – apreciar petições em face do operador de sistema de inteligência artificial após comprovada apresentação de reclamação não solucionada no prazo estabelecido em regulamentação; e
XIII – elaborar relatórios anuais acerca de suas atividades.	XIII – elaborar relatórios anuais acerca de suas atividades.
	[incluir inciso] — realizar auditoria de sistemas de inteligência artificial quando necessária para a aferição de conformidade com esta Lei, independente de segredo industrial;
	[incluir inciso] — determinar ao agente de inteligência artificial que realize auditoria externa e independente para avaliação do cumprimento do disposto nesta Lei, e na regulamentação;
	[incluir inciso] — credenciar instituições de pesquisa, mediante critérios estabelecidos em regulamento sujeito a consulta pública, para acesso a dados de auditorias.
	§ 2° Tanto a autoridade competente quanto eventuais entidades por ela credenciadas para realização de auditoria devem cumprir requisitos de segurança e confidencialidade das informações e de proteção de dados pessoais, nos termos da Lei n° 13.709, de 14 de agosto de 2018, e observar os segredos comercial e industrial.
	§ 3° As auditorias realizadas nos termos desta Lei devem proteger adequadamente os direitos e interesses legítimos a que se destinam, não podendo exigir acessos que violem a proteção de dados pessoais, segredos comerciais e industriais e outras informações confidenciais dos provedores e de quaisquer outras partes envolvidas, incluindo os destinatários do serviço, salvo quando estritamente necessárias para aferição de conformidade com esta Lei por parte da autoridade competente em casos em que houver fundada suspeita de violação legal.
Parágrafo único. Ao exercer as atribuições do caput, o órgão competente poderá estabelecer condições, requisitos, canais de comunicação e divulgação diferenciados para fornecedores e operadores de sistemas de inteligência artificial qualificados como micro ou pequenas empresas, nos termos da Lei Complementar n° 123, de 14 de dezembro de 2006, e startups, nos termos da Lei Complementar n° 182, de 1° de junho de 2021.	~~Parágrafo único.~~ § 4° Ao exercer as atribuições do caput, o órgão competente poderá estabelecer condições, requisitos, canais de comunicação e divulgação diferenciados para fornecedores e operadores de sistemas de inteligência artificial qualificados como micro ou pequenas empresas, nos termos da Lei Complementar n° 123, de 14 de dezembro de 2006, e startups, nos termos da Lei Complementar n° 182, de 1° de junho de 2021.

sugestão de redação ~~sugestão de exclusão~~

d) Sistemas utilizados pelo poder público

A definição das responsabilidades em termos de transparência também é vaga no texto, na medida que propõe disposições que incidam simultaneamente sobre o uso de IA pelo poder público e pelo setor privado.

Nos casos de desenvolvimento, aquisição e emprego de IA pelo **poder público**, é essencial que a transparência esteja **embasada na Lei de Acesso à Informação**, no sentido de haver um **rol de informações mínimas** que seja garantido às pessoas em transparência ativa, e não somente ao usuário ou "pessoa diretamente afetada" mediante requisição como o artigo 7º propõe.

Ademais, compete sublinhar que a **publicidade é um dos princípios que rege a Administração Pública**, nos termos do artigo 37 da Constituição Federal . No mesmo contexto, o artigo 5º, inciso XXXIII, da Constituição Federal, dispõe que "todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestados no prazo da lei, sob pena de responsabilidade".

Nesse sentido, as informações que devem ser providas em transparência ativa pelo poder público a respeito desses sistemas envolvem, pelo menos:

a. **descrição do sistema**, o que inclui informações sobre quais técnicas estão envolvidas no funcionamento da tecnologia, informações operacionais, lógica de seu funcionamento e quais categorias de dados são por eles tratados;

b. **potenciais riscos**;

c. **entidade fornecedora do sistema**;

d. **entidade da administração pública que faz uso do sistema**;

e. **forma de aquisição e valor**;

f. informação de quais entidades têm ou possam vir a ter **acesso aos dados** tratados pelo sistema;

g. se forem de alto risco, a **Avaliação de Impacto Algorítmico**;

h. quantificação de **gastos energéticos** dispendidos pelo sistema desde o início de seu ciclo de vida;

i. mecanismos para **contestar** o uso desses sistemas, inclusive para solicitar revisão humana ou para exercitar qualquer dos direitos previstos na lei;

j. quaisquer **outras informações** que já sejam objeto de leis, como a Lei Geral de Proteção de Dados ou a Lei de Acesso à Informação.

Também cabe destacar, no caso do poder público, a necessidade de inclusão no texto de instrumentos legais que garantam a **transparência sobre os sistemas de IA como um todo**, especialmente quando por ele empregados. Isso engloba a abertura das bases de dados utilizadas para treinamento e validação, com anonimização quando os dados pessoais puderem identificar uma pessoa; a transparência dos códigos dos algoritmos desenvolvidos ou contratados, que no caso do poder público devem ser prioritariamente soluções de código aberto; e a transparência sobre os processos de aquisição ou desenvolvimento e seus responsáveis.

Para casos que envolvam a contratação de sistemas protegidos por sigilo comercial, o poder público deve informar pelo menos as variáveis de entrada e saída do modelo, bem como o tipo de algoritmo utilizado, e promover auditorias periódicas sobre eles com especialistas externos ao órgão responsável, publicando o relatório resultante em transparência ativa. Para tanto, a presença de um **órgão ou setor de um órgão para avaliar sistemas e receber queixas sobre eles** pode ser uma medida eficaz.

Recomendamos, portanto, a seguinte redação:

REDAÇÃO ORIGINAL	*REDAÇÃO SUGERIDA
sem correspondência; incluir	Art. [ ] O órgão do poder público que desenvolver ou aplicar sistema de inteligência artificial deverá tornar disponíveis, via mecanismo de transparência ativa em seu sítio eletrônico, as seguintes informações sobre o sistema: I — descrição do sistema, incluindo informações sobre quais técnicas estão envolvidas no funcionamento da tecnologia, informações operacionais, lógica de seu funcionamento e quais categorias de dados são por eles tratados; II — potenciais riscos; III — entidade fornecedora do sistema; IV — entidade da administração pública que faz uso do sistema; V — forma de aquisição e valor; VI — informação de quais entidades têm ou possam vir a ter acesso a dados pessoais tratados pelo sistema; VII — se forem de alto risco, a Avaliação de Impacto Algorítmico; VIII - quantificação de gastos energéticos dispendidos pelo sistema desde o início de seu ciclo de vida; IX — mecanismos para que pessoas afetadas possam contestar o uso desses sistemas, inclusive para solicitar revisão humana ou para exercitar qualquer dos direitos previstos nesta lei; e X — quaisquer outras informações a serem publicizadas conforme o disposto em outras leis, como a Lei Geral de Proteção de Dados Pessoais ou a Lei de Acesso à Informação.

sugestão de redação ~~sugestão de exclusão~~

e) Informações sobre impactos ambientais

Sistemas de IA têm impactos ambientais expressivos, que compreendem o consumo de energia para seu treinamento, de água para resfriamento de CPUs em data centers que onde bases de dados de treinamento são processadas, de minério para construir equipamentos como celulares e computadores em que esses sistemas operam. Como exemplo, um data center que a Google constrói no Uruguai consumirá, por dia, até 7,6 milhões de litros de água por dia nos dias de verão. Esse volume não é desprezível, eis que corresponde ao consumo diário de água potável de 55 mil pessoas[32].

Ocorre que as informações a respeito da quantidade efetiva dos recursos que são consumidos ainda são insuficientes para compreender qual é, de fato, a magnitude do impacto ambiental que envolve o ecossistema do desenvolvimento, operação e descarte desses sistemas.

Por isso, é fundamental que o projeto de lei traga obrigações específicas para fornecimento de informações, de forma pública, facilmente acessível e compreensível pela população, a respeito do impacto ambiental de seu produto, de modo a incluir, no mínimo, informações sobre o consumo de energia do sistema ou grupo de sistemas utilizados. Informações sobre quais os equipamentos usados e onde são hospedados os dados tratados, de modo a permitir o mapeamento do consumo de recursos minerais e água, também são plenamente cabíveis de serem exigidas. É o que já fazem, inclusive, emendas apresentadas pelo Parlamento Europeu em seu posicionamento a respeito da regulação europeia de IA, o AI Act[33].

A mensuração desses dados deve ser conduzida e publicizada durante todo seu ciclo de vida, o que inclui concepção, desenvolvimento, operação, modificação e, no caso de equipamentos físicos, de descarte.

32 MÉNDEZ, Camila. Data center de Google podría utilizar un máximo de 7.600.000 litros de agua potable por día. La diaria ambiente. Disponível em: https://ladiaria.com.uy/ambiente/articulo/2023/3/data-center-de-google-podria-utilizar-un-maximo-de-7600000-litros-de-agua-potable-por-dia/. Acesso em: 04 jul. 2023.

33 PARLAMENTO EUROPEU. Disponível em: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html. Acesso em: 05 jul. 2023.

Tudo isso está de acordo, inclusive, com o disposto no Acordo de Escazú, assinado pelo Brasil em 2018, e encaminhado[34] em maio deste ano pela Presidência da República para ratificação pelo Congresso Nacional. O Acordo traz, em seu artigo 1º, obrigações específicas para implementação dos "direitos de acesso à informação ambiental, participação pública nos processos de tomada de decisões ambientais e acesso à justiça em questões ambientais". Também está em consonância com o artigo 225 da Constituição Federal, que estabelece o direito fundamental ao meio ambiente ecologicamente equilibrado e com os Objetivos de Desenvolvimento Sustentável estabelecidos pela Assembleia Geral das Nações Unidas.

REDAÇÃO ORIGINAL	*REDAÇÃO SUGERIDA
sem correspondência; incluir	Art. [ ] Agentes de inteligência artificial devem documentar e disponibilizar os parâmetros relativos aos impactos ambientais causados por seus sistemas, incluindo o consumo de recursos como energia, água, dentre outros, resultante do projeto, do gerenciamento de dados, do treinamento e das infraestruturas subjacentes do sistema de inteligência artificial, bem como os métodos adotados pelo agente para reduzir esse impacto.

sugestão de redação ~~sugestão de exclusão~~

34 BRASIL. Governo envia Acordo de Escazú para o Congresso. Disponível em: https://www.gov.br/mma/pt-br/assuntos/noticias/governo-envia-acordo-de-escazu-para-o-congresso. Acesso em: 05 jul. 2023.

6 CATEGORIZAÇÃO DE RISCOS

Alguns sistemas de IA podem violar frontalmente direitos fundamentais, vulnerabilizando a subsistência, a segurança e a integridade física e mental das pessoas. Nesses casos, os riscos são difíceis de evitar, mitigar ou compensar, razão pela qual se caracterizam como expressivos e desproporcionais. **Estes são classificados como riscos inaceitáveis, devendo seu uso ser banido da sociedade.**

Dito isso, a **primeira hipótese** de risco inaceitável, em que o uso de sistemas de IA deve ser banido, está ligada às tecnologias de **reconhecimento biométrico e facial** para promoção de vigilância em massa no **para atividades de segurança pública**, seja em retrospectiva ou em tempo real. A baixa acurácia atrelada aos vieses raciais encontrados nessa tecnologia, bem como o histórico racista das bases de dados de pessoas procuradas pela polícia e que alimentam esses sistemas, aumentam a ocorrência da discriminação — ou mesmo racismo — algorítmica[35]. Além disso, a coleta de dados biométricos e seu uso em ferramentas de estatísticas tendem a criar um ciclo retroalimentativo de marginalização de grupos vulneráveis, já que sistemas de IA se alimentam de dados que são historicamente enviesados pelo racismo estrutural[36].

Ainda, conforme já disposto em Carta Aberta da Access Now sobre a temática, "enquanto as pessoas em espaços acessíveis ao público puderem ser instantaneamente identificadas, destacadas ou rastreadas, seus direitos humanos serão minados"[37], uma vez que a vigilância constante e desmotivada (sem justa causa em relação à pessoa que está sendo identificada) inibe que o indivíduo exerça livremente seus direitos e, inclusive, desenvolva sua personalidade.

Nessa mesma linha, pode-se ainda citar o **policiamento preditivo**[38], cujo propósito seria o de usar e analisar dados para monitoramento e identificação de situações

35 ACCESS NOW. **Carta aberta para banimento global de usos de reconhecimento facial e outros reconhecimentos biométricos remotos que permitam vigilância em massa, discriminatória e enviesada.** 2021. Disponível em: https://www.accessnow.org/cms/assets/uploads/2021/06/BanBS-Portuguese.pdf. p. 3. Acesso em: 03 jul. 2023.

36 EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS. **Bias in algorithms - Artificial intelligence and discrimination.** Disponível em: https://fra.europa.eu/en/publication/2022/bias-algorithm. Acesso em: 03 jul. 2023.

37 ACCESS NOW. **Carta aberta para banimento global de usos de reconhecimento facial e outros reconhecimentos biométricos remotos que permitam vigilância em massa, discriminatória e enviesada.** 2021. Disponível em: https://www.accessnow.org/cms/assets/uploads/2021/06/BanBS-Portuguese.pdf. p. 3. Acesso em: 03 jul. 2023.

38 "Aplicação da modelagem por computadores a dados criminais passados para predizer atividade criminal futura". JOH, E. E. **Policing by numbers: Big data and the 4th Amendment.** Washington Law Review, v. 89, 2014. Disponível em: https://digitalcommons.law.uw.edu/cgi/viewcontent.cgi?article=4797&context=wlr. Acesso em: 03 jul. 2023.

suspeitas. Por serem sistemas baseados em conjuntos de dados originariamente opacos, racistas e inconsistentes, seu uso, além de não haver comprovação alguma de benefício para a segurança pública, da mesma forma aumenta a vigilância, práticas discriminatórias e reforça desigualdades socioeconômicas. A experiência de outros países trouxe consequências de grande impacto, como o aumento exponencial de abordagens policiais (aumento da vigilância), restrições às liberdades individuais, despejos, desempregos, evasão/expulsão de escolas, e aumento da desconfiança com os serviços públicos[39].

Nesse ponto, o **artigo 17, incisos XI e XII, do PL nº 2338/2023**, traz a disposição de que são considerados sistemas de inteligência artificial de **alto risco** aqueles utilizados para as finalidades de investigação criminal e segurança pública, bem como estudo analítico de crimes relativos a pessoas naturais[40].

A inclusão desse dispositivo, no sentido de determinar que tais sistemas serão considerados de alto risco quando utilizados para tais finalidades, culmina por chancelar a possibilidade dessa utilização.

Ocorre, contudo, que **tal risco é inaceitável**[41].

Avaliações individuais de risco de cometer infrações ou de reincidir, ou, ainda, para avaliar traços de personalidade e características ou comportamento criminal de pessoas ou grupos não deveriam ser delegadas a uma IA. Ressalte-se que a avaliação da personalidade do agente criminoso pode caracterizar o nocivo fenômeno do Direito Penal do Inimigo[42], incompatível com a axiologia da CF/88, eis que o réu não pode ser punido pelo que é, mas pelo que faz.

Afinal, essas ferramentas permitem a **automatização de práticas racistas** pelo sistema penal de modo a agravar o encarceramento em massa da população negra

---

39 GOMES, Letícia Simões. Policiamento preditivo, controle social e desigualdades raciais. Disponível em: https://anpocs.com/index.php/encontros/papers/43-encontro-anual-da-anpocs/spg-6/spg32-1/12010-policiamento-preditivo-controle-social-e-desigualdades-raciais. Acesso em: 10 jul. 2023.

40 XI – investigação criminal e segurança pública, em especial para avaliações individuais de riscos pelas autoridades competentes, a fim de determinar o risco de uma pessoa cometer infrações ou de reincidir, ou o risco para potenciais vítimas de infrações penais ou para avaliar os traços de personalidade e as características ou o comportamento criminal passado de pessoas singulares ou grupos; XII – estudo analítico de crimes relativos a pessoas naturais, permitindo às autoridades policiais pesquisar grandes conjuntos de dados complexos, relacionados ou não relacionados, disponíveis em diferentes fontes de dados ou em diferentes formatos de dados, no intuito de identificar padrões desconhecidos ou descobrir relações escondidas nos dados.

41 Conforme inclusive reconhecido pelo Parlamento Europeu em votação de 11 de maio de 2023, que proibiu o uso de policiamento preditivo e sistemas criminais de predição. Disponível em: https://www.fairtrials.org/articles/news/eu-parliament-votes-for-landmark-ban/. Acesso em: 03 jul. 2023.

42 GRECO, Luís. **Sobre o chamado Direito Penal do Inimigo**. Revista da Faculdade de Direito de Campos. Ano VI, Nº 7, 2005. Disponível em: http://fdc.br/arquivos/mestrado/revistas/revista07/docente/07.pdf. Acsso em: 03 jul. 2023.

no Brasil. Nos Estados Unidos, por exemplo, o caso ProPublica denunciou como essas ferramentas — um sistema de quantificação da probabilidade de incidência de detentos — são enviesadas, a ponto de considerar pessoas negras mais passíveis de reincidência do que brancas mesmo com estatísticas a provar o contrário[43].

Erros cometidos por mecanismos de reconhecimento facial podem significar que uma pessoa inocente será seguida, investigada, e até mesmo presa e condenada por um crime que não cometeu. Um erro de um sistema de reconhecimento facial em câmeras corporais pode ser letal: um policial, alerta a uma potencial ameaça, pode decidir em um instante para onde apontar sua arma. Em mais um exemplo comparado, trazemos que as autoridades policiais do País de Gales testaram a vigilância por escaneamento facial em mais de uma dúzia de eventos públicos. Durante a maioria deles, o número de falsas "correspondências" registradas pelo sistema excedeu em muito o número de suspeitos identificados. Em um teste, mais de 9 de cada 10 alertas que o sistema de IA enviou à polícia sobre uma possível correspondência criminal - de quase 2.500 no total - foram alertas acionados pelo rosto de uma pessoa inocente[44].

Por isso, devem os casos apresentados nos incisos XI e XII, do artigo 17º, serem considerados riscos inaceitáveis, e não altos, de modo a **efetivamente banir a possibilidade de policiamento preditivo no Brasil, na mesma linha de diversas experiências internacionais**[45].

O texto do PL nº 2338/2023 também traz contradições internas e interpretações incompatíveis com a sistemática do ordenamento jurídico no que tange ao uso da tecnologia na segurança pública. Isso porque o **artigo 15** dispõe que, no âmbito de atividades de **segurança pública, somente é permitido o uso de sistemas de identificação biométrica à distância**, de forma contínua em espaços acessíveis ao público, quando houver previsão em lei federal específica e autorização judicial em

---

43 LARSON, J. et al. **How We Analyzed the COMPAS Recidivism Algorithm.** Pro Publica. 2016. Disponível em: https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm; EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS. **Bias in algorithms - Artificial intelligence and discrimination.** Viena, 2022. Disponível em: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2022-bias-in-algorithms_en.pdf. Acesso em: 03 jul. 2023.

44 GARVIE, Claire. **Facial recognition threatens our fundamental rights.** The Washington Post. Disponível em:https://www.washingtonpost.com/opinions/facial-recognition-threatens-our-fundamental-rights/2018/07/19/a102703a-8b64-11e8-8b20-60521f27434e_story.html. Acesso em: 03 jul. 2023.

45 BRADY, Gary. **Germany says no to predictive policing – the rule of law challenges posed by algorithms.** EMILDAI. Disponível em: https://emildai.eu/germany-says-no-to-predictive-policing-the-rule-of-law-challenges-posed-by-algorithms/. Acesso em: 03 jul. 2023. FAIRS TRIAL. **EU Parliament votes for landmark ban on "discriminatory and unjust" predictive policing and criminal prediction systems.** Disponível em: https://www.fairtrials.org/articles/news/eu-parliament-votes-for-landmark-ban/. Acesso em: 03 jul. 2023. MILLER, Susan. **Santa Cruz bans predictive policing.** GCN. Disponível em: https://gcn.com/data-analytics/2020/07/santa-cruz-bans-predictive-policing/315055/. Acesso em: 03 jul. 2023.

conexão com a atividade de persecução penal individualizada, nos casos de persecução de crimes passíveis de pena máxima de reclusão superior a dois anos, busca de vítimas de crimes ou pessoas desaparecidas ou nos casos de crime em flagrante.

Além disso, o dispositivo promove a vigilância massiva ao abrir espaço para o armazenamento indiscriminado de imagens, considerando que poderão não ser deletadas de forma indeterminada pela mera expectativa de um dia poderem ser utilizadas. Afeta, portanto, o direito à privacidade e à proteção de dados pessoais, além do direito à livre associação, a poder criar um efeito inibitório que tornará as pessoas sempre temerosas de promover sua cidadania em espaços públicos por meio de manifestações, por exemplo, pelo fato de se sentirem vigiadas. **Trata-se, portanto, de medida desproporcional, que privilegia um ambiente de constante e excessivo monitoramento, além de estar em dissonância com a axiologia protetiva da LGPD.**

Adicionalmente, a prisão em flagrante é incompatível com a concessão de prévia autorização judicial e dispensa a expedição de lei federal específica. Nesse ponto, o artigo 5º, LXI, da CF/88 determina que ninguém será preso senão em flagrante delito ou por ordem escrita e fundamentada de autoridade judiciária competente, concluindo que na prisão em flagrante não há necessidade de ordem escrita e fundamentada de autoridade competente. No mesmo sentido, o artigo 301 do Código de Processo Penal dispõe que as autoridades policiais, seus agentes ou qualquer do povo poderá prender quem quer que seja encontrado em flagrante delito. **O artigo 15 do PL nº 2338/2023, portanto, cria hipótese legal que já nasceria inconstitucional.**

O argumento de que o uso do reconhecimento facial na segurança pública seria supervisionado dentro das estruturas organizacionais com treinamento adequado voltado à tecnologia empregada e com responsabilidade humana por eventuais erros e excessos também **não é suficiente para mitigar a incompatibilidade do uso dessa tecnologia com a Constituição Federal por sua massiva capacidade discriminatória**. Tal abordagem não é compatível com o princípio precaucionário que disciplina a temática e que também está expressamente previsto no artigo 3º, inciso XI, do PL nº 2338/2023.

Compreende-se, então, que **o uso dessas tecnologias de reconhecimento facial e de policiamento preditivo deve ser banido**, pois, caso contrário, estaremos promovendo ferramentas que fomentam a vigilância, a cultura do encarceramento de populações negras e vulneráveis e do punitivismo do sistema penal.

A **segunda hipótese de risco inaceitável** é o investimento e o desenvolvimento de sistemas autônomos letais com potencial de causar morte em um confronto armado. Além de serem sistemas cuja finalidade por si só não é neutra, colocando o direito fundamental mais caro em risco, há mínima interferência de um ser humano no poder decisório e impossibilidade de exigir total responsabilização de quem os opera.

A **terceira hipótese** está ligada ao uso de sistemas de IA que se valem de vulnerabilidades físicas, emocionais e psicológicas para distorcer e manipular o comportamento de indivíduos ou grupo de indivíduos[46], **como o reconhecimento de emoções**. Além dos riscos inerentes ao uso da IA para este fim, não há qualquer fundamento científico de que seja possível identificar emoções somente com base em expressões faciais[47].

Sugere-se, portanto, a exclusão do parágrafo segundo do artigo 7º do PL nº 2338/2023, que determina que "pessoas expostas a sistemas de reconhecimento de emoções ou a sistemas de categorização biométrica serão informadas sobre a utilização e o funcionamento do sistema no ambiente em que ocorrer a exposição". Essa disposição culmina por admitir o uso de sistemas de reconhecimento de emoções ou categorização biométrica, desde que sejam informadas sobre essa utilização. No entanto, compreende-se que esse uso é nocivo à adequada tutela dos direitos fundamentais, especialmente por violar a intimidade do indivíduo (art. 5º, X, CF/1988).

Por fim, a **quarta hipótese de risco inaceitável** refere-se ao uso de sistemas de IA que valoram a confiança de um indivíduo ou de um grupo de indivíduos mediante análise de conduta social ou de características pessoais ou de personalidade (conhecidas ou preditivas), causando um tratamento prejudicial ou desfavorável capaz de injustamente limitar ou impossibilitar o regular exercício de direitos, c**omo o crédito social** (social scoring)[48] - **hipótese prevista no artigo 14, inciso III, do PL nº 2338/2023**[49].

---

46 COMISSÃO EUROPEIA. **Proposta de regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de Inteligência Artificial (Regulamento Inteligência Artificial) e altera determinados atos legislativos da União**. 2021. Artigo 5°. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52021PC0206. Acesso em: 03 jul. 2023.

47 BARRET, L. F. et al. **Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements**. Psychological Science in the Public Interest, 20(1), 1–68, 2019. Disponível em: https://doi.org/10.1177/1529100619832930. Acesso em: 03 jul. 2023.

48 idem.

49 Art. 14. **São vedadas** a implementação e o uso de sistemas de inteligência artificial: I – que empreguem técnicas subliminares que tenham por objetivo ou por efeito induzir a pessoa natural a se comportar de forma prejudicial ou perigosa à sua saúde ou segurança ou contra os fundamentos desta Lei; II – que explorem quaisquer vulnerabilidades de grupos específicos de pessoas naturais, tais como as associadas a sua idade ou deficiência física ou mental, de modo a induzi-las a se comportar de forma prejudicial a sua saúde ou segurança ou contra os fundamentos desta Lei; III – **pelo poder público, para avaliar, classificar ou ranquear as pessoas naturais, com base no seu comportamento social ou em atributos da sua personalidade, por meio de pontuação universal, para o acesso a bens e serviços e políticas públicas, de forma ilegítima ou desproporcional** (nosso grifo).

Assim, pode-se citar como sistemas de IA que geram riscos inaceitáveis, devendo ser banidos no ordenamento jurídico brasileiro, as aplicações para reconhecimento facial em espaços públicos, policiamento preditivo, sistemas autônomos letais, reconhecimento de emoções e crédito social (social scoring). No entanto, vale ressaltar que outros casos os quais o uso deva ser banido podem surgir com o tempo. Sugere-se, portanto, que a futura legislação preveja a possibilidade de adição de novos casos pela autoridade competente.

REDAÇÃO ORIGINAL	REDAÇÃO SUGERIDA
Art. 14. São vedadas a implementação e o uso de sistemas de inteligência artificial:	**Art. 14.** São vedadas a implementação e o uso de sistemas de inteligência artificial:
I – que empreguem técnicas subliminares que tenham por objetivo ou por efeito induzir a pessoa natural a se comportar de forma prejudicial ou perigosa à sua saúde ou segurança ou contra os fundamentos desta Lei;	I – que empreguem técnicas subliminares que tenham por objetivo ou por efeito induzir a pessoa natural a se comportar de forma prejudicial ou perigosa à sua saúde ou segurança ou contra os fundamentos desta Lei;
II – que explorem quaisquer vulnerabilidades de grupos específicos de pessoas naturais, tais como as associadas a sua idade ou deficiência física ou mental, de modo a induzi-las a se comportar de forma prejudicial a sua saúde ou segurança ou contra os fundamentos desta Lei;	II – que explorem quaisquer vulnerabilidades de grupos específicos de pessoas naturais, tais como as associadas a sua idade ou deficiência física ou mental, de modo a induzi-las a se comportar de forma prejudicial a sua saúde ou segurança ou contra os fundamentos desta Lei;
III – pelo poder público, para avaliar, classificar ou ranquear as pessoas naturais, com base no seu comportamento social ou em atributos da sua personalidade, por meio de pontuação universal, para o acesso a bens e serviços e políticas públicas, de forma ilegítima ou desproporcional.	III – pelo poder público, para avaliar, classificar ou ranquear as pessoas naturais, com base no seu comportamento social ou em atributos da sua personalidade, por meio de pontuação universal, para o acesso a bens e serviços e políticas públicas, de forma ilegítima ou desproporcional.
	[incluir inciso] - que reconheça emoções;
	[incluir inciso] - o uso de sistemas de identificação biométrica para atividades de segurança pública, seja em tempo real ou em retrospectiva;
	[incluir inciso] – o uso de sistemas de inteligência artificial para fins de investigação criminal e segurança pública que façam avaliações individuais de risco de uma pessoa cometer infrações ou de reincidir, ou para avaliar os traços de personalidade e as características ou o comportamento criminal passado de pessoas singulares ou grupos;
	[incluir inciso] – o uso de sistemas de inteligência artificial para realizar estudo analítico de crimes relativos a pessoas naturais;
	[incluir inciso] - o uso de sistemas autônomos letais.
Art. 15. No âmbito de atividades de segurança pública, somente é permitido o uso de sistemas de identificação biométrica à distância, de forma contínua em espaços acessíveis ao público, quando houver previsão em lei federal específica e autorização judicial em conexão com a atividade de persecução penal individualizada, nos seguintes casos:	~~Art. 15. No âmbito de atividades de segurança pública, somente é permitido o uso de sistemas de identificação biométrica à distância, de forma contínua em espaços acessíveis ao público, quando houver previsão em lei federal específica e autorização judicial em conexão com a atividade de persecução penal individualizada, nos seguintes casos:~~
I – persecução de crimes passíveis de pena máxima de reclusão superior a dois anos;	~~I – persecução de crimes passíveis de pena máxima de reclusão superior a dois anos;~~

sugestão de redação ~~sugestão de exclusão~~

REDAÇÃO ORIGINAL	REDAÇÃO SUGERIDA
II – busca de vítimas de crimes ou pessoas desaparecidas; ou	~~II – busca de vítimas de crimes ou pessoas desaparecidas; ou~~
III – crime em flagrante.	~~III – crime em flagrante.~~
Parágrafo único. A lei a que se refere o caput preverá medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal e o controle judicial, bem como os princípios e direitos previstos nesta Lei, especialmente a garantia contra a discriminação e a necessidade de revisão da inferência algorítmica pelo agente público responsável, antes da tomada de qualquer ação em face da pessoa identificada.	~~Parágrafo único. A lei a que se refere o caput preverá medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal e o controle judicial, bem como os princípios e direitos previstos nesta Lei, especialmente a garantia contra a discriminação e a necessidade de revisão da inferência algorítmica pelo agente público responsável, antes da tomada de qualquer ação em face da pessoa identificada.~~
Art. 17. São considerados sistemas de inteligência artificial de alto risco aqueles utilizados para as seguintes finalidades:	Art. 17. São considerados sistemas de inteligência artificial de alto risco aqueles utilizados para as seguintes finalidades:
I – aplicação como dispositivos de segurança na gestão e no funcionamento de infraestruturas críticas, tais como controle de trânsito e redes de abastecimento de água e de eletricidade;	I – aplicação como dispositivos de segurança na gestão e no funcionamento de infraestruturas críticas, tais como controle de trânsito e redes de abastecimento de água e de eletricidade;
II – educação e formação profissional, incluindo sistemas de determinação de acesso a instituições de ensino ou de formação profissional ou para avaliação e monitoramento de estudantes;	II – educação e formação profissional, incluindo sistemas de determinação de acesso a instituições de ensino ou de formação profissional ou para avaliação e monitoramento de estudantes;
III – recrutamento, triagem, filtragem, avaliação de candidatos, tomada de decisões sobre promoções ou cessações de relações contratuais de trabalho, repartição de tarefas e controle e avaliação do desempenho e do comportamento das pessoas afetadas por tais aplicações de inteligência artificial nas áreas de emprego, gestão de trabalhadores e acesso ao emprego por conta própria;	III – recrutamento, triagem, filtragem, avaliação de candidatos, tomada de decisões sobre promoções ou cessações de relações contratuais de trabalho, repartição de tarefas e controle e avaliação do desempenho e do comportamento das pessoas afetadas por tais aplicações de inteligência artificial nas áreas de emprego, gestão de trabalhadores e acesso ao emprego por conta própria;
IV – avaliação de critérios de acesso, elegibilidade, concessão, revisão, redução ou revogação de serviços privados e públicos que sejam considerados essenciais, incluindo sistemas utilizados para avaliar a elegibilidade de pessoas naturais quanto a prestações de serviços públicos de assistência e de seguridade;	IV – avaliação de critérios de acesso, elegibilidade, concessão, revisão, redução ou revogação de serviços privados e públicos que sejam considerados essenciais, incluindo sistemas utilizados para avaliar a elegibilidade de pessoas naturais quanto a prestações de serviços públicos de assistência e de seguridade;
V – avaliação da capacidade de endividamento das pessoas naturais ou estabelecimento de sua classificação de crédito;	V – avaliação da capacidade de endividamento das pessoas naturais ou estabelecimento de sua classificação de crédito;
VI – envio ou estabelecimento de prioridades para serviços de resposta a emergências, incluindo bombeiros e assistência médica;	VI – envio ou estabelecimento de prioridades para serviços de resposta a emergências, incluindo bombeiros e assistência médica;
VII – administração da justiça, incluindo sistemas que auxiliem autoridades judiciárias na investigação dos fatos e na aplicação da lei;	VII – administração da justiça, incluindo sistemas que auxiliem autoridades judiciárias na investigação dos fatos e na aplicação da lei;
VIII – veículos autônomos, quando seu uso puder gerar riscos à integridade física de pessoas;	VIII – veículos autônomos, quando seu uso puder gerar riscos à integridade física de pessoas;
IX – aplicações na área da saúde, inclusive as destinadas a auxiliar diagnósticos e procedimentos médicos;	IX – aplicações na área da saúde, inclusive as destinadas a auxiliar diagnósticos e procedimentos médicos;
X – sistemas biométricos de identificação;	X – sistemas biométricos de identificação;

sugestão de redação ~~sugestão de exclusão~~

REDAÇÃO ORIGINAL	REDAÇÃO SUGERIDA
XI – investigação criminal e segurança pública, em especial para avaliações individuais de riscos pelas autoridades competentes, a fim de determinar o risco de uma pessoa cometer infrações ou de reincidir, ou o risco para potenciais vítimas de infrações penais ou para avaliar os traços de personalidade e as características ou o comportamento criminal passado de pessoas singulares ou grupos;	~~XI – investigação criminal e segurança pública, em especial para avaliações individuais de riscos pelas autoridades competentes, a fim de determinar o risco de uma pessoa cometer infrações ou de reincidir, ou o risco para potenciais vítimas de infrações penais ou para avaliar os traços de personalidade e as características ou o comportamento criminal passado de pessoas singulares ou grupos;~~
XII – estudo analítico de crimes relativos a pessoas naturais, permitindo às autoridades policiais pesquisar grandes conjuntos de dados complexos, relacionados ou não relacionados, disponíveis em diferentes fontes de dados ou em diferentes formatos de dados, no intuito de identificar padrões desconhecidos ou descobrir relações escondidas nos dados;	~~XII – estudo analítico de crimes relativos a pessoas naturais, permitindo às autoridades policiais pesquisar grandes conjuntos de dados complexos, relacionados ou não relacionados, disponíveis em diferentes fontes de dados ou em diferentes formatos de dados, no intuito de identificar padrões desconhecidos ou descobrir relações escondidas nos dados;~~
XIII – investigação por autoridades administrativas para avaliar a credibilidade dos elementos de prova no decurso da investigação ou repressão de infrações, para prever a ocorrência ou a recorrência de uma infração real ou potencial com base na definição de perfis de pessoas singulares; ou	XIII – investigação por autoridades administrativas para avaliar a credibilidade dos elementos de prova no decurso da investigação ou repressão de infrações, para prever a ocorrência ou a recorrência de uma infração real ou potencial com base na definição de perfis de pessoas singulares; ou
XIV – gestão da migração e controle de fronteiras.	XIV – gestão da migração e controle de fronteiras.

sugestão de redação ~~sugestão de exclusão~~

7 AUTORIDADE COMPETENTE

I. Natureza jurídica

O PL determina, em seu **artigo 32**, que o "Poder Executivo designará autoridade competente para zelar pela implementação e fiscalização da presente Lei".

A criação de entidade central responsável pela fiscalização da lei é **bem-vinda**, e permitirá uma centralização maior da interpretação da futura lei a ser aprovada, de modo a atuar como um farol direcionador de agentes de IA para que adotem práticas que sejam mais protetivas de direitos durante o ciclo de vida de seus sistemas.

Justamente por esse papel central, é fundamental que a autoridade tenha **natureza autárquica**, de modo a ter independência financeira, orçamentária, funcional e administrativa que lhe proteja o exercício pleno de suas funções de intimidações de outros atores, sejam públicos ou privados. Nesse ponto, sugere-se que o artigo 32 já mencione a independência da autoridade competente, viabilizando a sua posterior implementação pelo Poder Executivo.

Isso é de especial significado considerando que será a autoridade em questão responsável também por supervisionar outros órgãos do poder público. Por isso, é fundamental que tenha as prerrogativas necessárias para cumprir suas funções de forma autônoma, de modo a se proteger de captura regulatória, seja pelo poder público ou privado, ao ter plenos poderes de supervisão, fiscalização e normatização de atividades.

Autonomia orçamentária e decisória (órgão máximo da autoridade como última instância), por sua vez, bem como a previsão de inamovibilidade de seus membros, são aspectos fundamentais para se estabelecer garantias contra a captura de autoridades reguladoras[50]. Exemplos nesse sentido de medidas que ampliam o multissetorialismo no âmbito de autoridade reguladora no Brasil encontram-se na Lei Geral de Proteção de Dados, que cabem ser replicados nesta proposta.

Em síntese, compreende-se que a autoridade competente deva gozar de **estabilidade dos dirigentes e de autonomia funcional, decisória, administrativa e financeira**. Também impende ressaltar a inviabilidade de interposição de recurso hierárquico impróprio de suas decisões, assegurando-lhe efetiva independência.

55 ARANHA, Márcio. Manual de Direito Regulatório: Fundamentos de Direito Regulatório. 4a Edição. London: Laccademia publishing, 2018, p. 36.

Por fim, impende ressaltar que, uma vez garantida a ampliação de suas competências, bem como de seu capital financeiro e quantidade e expertise de servidores, não vemos como problemática a ampliação do escopo de uma autoridade como a Autoridade Nacional de Proteção de Dados (ANPD).

II. Competências

Para além das competências já descritas pelo projeto de lei no artigo 32, é fundamental, como descrito acima, que a autoridade também tenha competência para **realizar auditoria** de sistemas de inteligência artificial, independentemente da existência de segredos industriais, **se houver fundado convencimento de poder infringir os dispositivo da lei**, inclusive aqueles relacionados aos direitos do sujeito afetado. Isso inclui também o poder de determinar o provimento de informações ao agente de IA no âmbito de processos administrativos que vier a abrir.

Para salvaguardar os interesses também dos agentes de IA, deve a autoridade ser, naturalmente, obrigada a garantir a proteção aos segredos industriais do agente, sob pena de responsabilização.

Adicionalmente, e também em referência ao já descrito na mesma seção acima sobre auditorias de sistemas de IA, propomos a inclusão de dispositivo que permita a **participação de entidades independentes especializadas no tema, seja de universidades, centros de pesquisa ou da sociedade civil organizada, na realização dessas auditorias e no acesso a informações sobre o funcionamento de sistemas de IA**. Isso poderá ser feito a partir do credenciamento, pela autoridade competente, dessas entidades para casos específicos e dentro dos limites que considerar cabíveis.

Em relação às competências da autoridade, também impende salientar a pertinência de convocação de consultas e audiências públicas, previamente à tomada de decisão, proposições de minutas e propostas de alteração de atos normativos de interesse geral sujeitos envolvidos.

No que tange ao **artigo 32, parágrafo único, VI**, que versa sobre a expedição de normas para a regulamentação da lei, também é sugerida a inclusão de alínea que preveja a atribuição de expedir normas para a regulamentação de procedimentos para a comunicação de incidentes graves, tais como aqueles que afetam gravemente direitos fundamentais, como a liberdade de expressão e privacidade, por exemplo.

8 SISTEMAS DE IA GENERATIVA

Os últimos meses foram marcados pelo lançamento no mercado de sistemas de IA generativa, também chamados de IA fundacional (foundation AI)[51], que têm sido amplamente divulgados pela mídia. É o caso de aplicações como ChatGPT, Stable Diffusion e Bing, capazes de criar conteúdo a partir de comandos escritos, comumente chamados de prompts.

De modo geral, esses sistemas podem ser utilizados para uma ampla variedade de tarefas e são desenvolvidos com base no tratamento de quantidades massivas de dados. Esses dados podem ser pessoais ou não, e serão aplicados para o treinamento dessas aplicações, de modo a criarem textos, imagens, vídeos e sons.

Por um lado, esses sistemas têm sido louvados pela **capacidade** que têm de agilizar processos e tornar, por assim dizer, mais produtivo o trabalho de seus usuários[52]. Por outro, têm sido objeto de **sensacionalismo**, inclusive por parte de seus próprios desenvolvedores[53], como parte de um projeto supostamente involuntário de avanço tecnológico que levaria ultimamente à extinção da humanidade.

Ocorre que, ofuscados por essas narrativas aparentemente opostas, estão uma série de **impactos que estes sistemas já causam**, muitos deles inclusive compartilhados com outras tecnologias baseadas em inteligência artificial mencionadas acima.

Esses impactos incluem, pelo menos: (i) imensa capacidade de esses sistemas serem usados em campanhas de desinformação; **(ii)** violações de proteção de dados pessoais; **(iii)** violações de direitos de propriedade intelectual; **(iv)** uso abusivo do conhecimento de povos tradicionais; **(v)** geração de conteúdo racista e sexista; **(vi)** massivo gasto energético e consumo de recursos naturais como minério e água para treinamento dessas tecnologias e para a construção e manutenção do equipamento em que seu desenvolvimento se dá; **(vii)** capacidade de facilitar a codificação de ferramentas que facilitam ataques cibernéticos; **(viii)** falhas de cibersegurança, que têm levado a expressivos vazamentos de dados — o Brasil, vale reiterar, foi o 3º

51 Sandford University Human-Centered Artificial Intelligence. Introducing the Center for Research on Foundation Models (CRFM). Disponível em: https://hai.stanford.edu/news/introducing-center-research-foundation-models-crfm. Acesso em: 02 jul. 2023.

52 TOKER, Erol. Como a inteligência artificial generativa vai impactar o futuro do trabalho. Fast Company Brasil. Disponível em: https://fastcompanybrasil.com/worklife/como-a-inteligencia-artificial-generativa-vai-impactar-o-futuro-do-trabalho/. Acesso em: 04 jul. 2023.

53 AFP RIO. Inteligência artificial vai substituir até 80% dos empregos e 'isso é bom', diz pesquisador. O Globo. Disponível em: https://oglobo.globo.com/economia/tecnologia/noticia/2023/05/inteligencia-artificial-vai-substituir-ate-80percent-dos-empregos-e-isso-e-bom-diz-pesquisador.ghtml. Acesso em: 04 jul. 2023.

país mais afetado no mundo por recente vazamento do ChatGPT; **(ix)** capacidade de aprofundar o epistemicídio do conhecimento produzido por populações não brancas, que estão fora da Minoria Global (também chamada de Norte Global), já que os discursos produzidos por esses sistemas se baseiam em dados que são extraídos principalmente dessa região, não representativos, portanto, das visões de mundo de outros povos; **(x)** exploração de trabalhadores pessimamente remunerados em países do Mundo Majoritário para fins de moderação de conteúdo nesses sistema.

Esses são alguns dos riscos apresentados por sistemas generativos, que **não podem deixar de ser endereçados por uma regulação efetiva de IA como a que se pretende ser o PL nº 2338/2023**. Algumas das obrigações presentes no PL já endereçam essas questões, mas salvaguardas adicionais devem ser incluídas.

A primeira deve referir-se à concessão, a reguladores e centros de pesquisa, de **acesso às bases de dados de treinamento utilizadas por esses sistemas**. Por mais que já se possa subsumir o acesso a bases de dados dentro das recomendações descritas nesta nota técnica, no caso de sistemas de IA generativa isso é fundamental para identificar de que modo atuam, tanto para reforçar a discriminação de populações historicamente marginalizadas, quanto para tirar lucros de trabalhos protegidos por propriedade intelectual. Tal tipo de transparência também pode servir para identificar de que modo seus desenvolvedores estão se beneficiando do conhecimento de povos tradicionais sem o devido reconhecimento ou compensação.

Neste ponto, como adendo, vale ressaltar a importância de se prever exceções para que sistemas de IA que sejam utilizados para fins de pesquisa, sem fins lucrativos, não estejam sujeitos ao pagamento de direitos de propriedade intelectual.

Para além disso, o provimento de informações a respeito de **gastos energéticos e outros impactos ambientais** deve ser garantido, nos termos do que já foi descrito nas seções anteriores. Sistemas generativos são conhecidos justamente por serem responsáveis por imensos gastos energéticos, considerando que um único sistema tem pegada de carbono similar a de quase cinco vezes as emissões de vida útil de um carro médio.

Vale considerar, ainda, a possibilidade de se criar a obrigação de que desenvolvedores de sistemas generativos criem técnicas para inclusão de marcas d'água no conteúdo gerado por essas aplicações. Apesar de esse ser um campo de estudo ainda em desenvolvimento, e que **marcas d'água** não podem ser vistas como uma bala de prata para identificar conteúdo gerado por IAs generativas por serem passíveis de burla, podem ser mais uma ferramenta contra, por exemplo, a automatização de desinformação por meio desses sistemas.

Compete também levar em conta os escândalos recentes que revelam como empresas como OpenAI, mas também outras grandes corporações de tecnologia como Amazon e Meta, têm **empregado trabalhadores do Sul Global, incluindo Brasil**, para realização de tarefas de catalogação de dados e moderação de conteúdo mediante remuneração e **condições de trabalho degradantes**. Isso foi inclusive revelado há poucas semanas pelo Intercept, que mostrou como esse tipo de trabalho afeta a saúde física e mental de indivíduos no Brasil e como a recompensa financeira de ter de assistir conteúdo violento tem sido por demais insatisfatória[54].

Levando em conta a complexidade dos interesses dos próprios trabalhadores que atuam nesses ambientes, talvez esta lei não seja o espaço para uma regulação desse serviço, motivo pelo qual uma legislação sobre trabalho vinculado a plataformas deve ser objeto de debate próprio.

Apesar disso, é fundamental compreender como as pessoas no Brasil estão sendo impactadas por essa prática e que relatórios sejam apresentados e publicizados, onde os desenvolvedores dessas tecnologias **descrevam de que forma houve o emprego de trabalhadores nessas funções**, seja via emprego imediato ou por meio da terceirização de sua força de trabalho. Tal descrição deve envolver, no mínimo, o **detalhamento** de **(i)** quantos trabalhadores foram empregados, **(ii)** para quais fins, **(iii)** mediante quais condições de trabalho, **(iv)** por qual remuneração, **(v)** qual foi a empresa intermediadora, se houve, e **(vi)** qual o perfil demográfico dessas pessoas, relacionados principalmente ao gênero e posição geográfica.

Por fim, ressaltamos a importância da promoção de debates no âmbito do Senado Federal a respeito dos impactos de sistemas de IA generativa e possíveis caminhos para remediá-los, adicionais aos aqui já mencionados, considerando o fato de serem ainda aplicações extremamente recentes. **A Coalizão Direitos na Rede se coloca à disposição para apoiar nessa discussão**.

54 RIBEIRO, Paulo Victor. Revolta, Impotência, Tristeza - Brasileiros ganham frações de centavos para melhorar sua inteligência artificial. The Intercept (2023). Disponível em: https://www.intercept.com.br/2023/06/19/brasileiros-ganham-fracoes-de-centavos-para-melhorar-sua-inteligencia-artificial/. Acesso em: 03 jul. 2023.

9 RESPONSABILIDADE CIVIL

No que tange à responsabilidade civil, verifica-se que o **Projeto de Lei n° 21-A/2020** previa, em seu **artigo 6º, VI**, de modo abstrato, a **responsabilidade subjetiva** como regra geral nos casos de inteligência artificial, desprestigiando a cláusula geral do risco prevista no **artigo 927 do Código Civil**[55], bem como a análise de caso concreto que norteia a operacionalização dos eventos de responsabilidade.

A previsão também vulnerabilizava diretrizes fundamentais como a solidariedade social e o direito da vítima à reparação integral de seus danos, caracterizando inegável retrocesso.

Ao restringir a responsabilidade somente à esfera subjetiva, o dispositivo desconsiderava que a avaliação da responsabilidade civil como subjetiva ou objetiva depende do caso concreto, notadamente quando se trata de inteligência artificial, cuja aplicação pode ocorrer nas formas e nos contextos mais distintos possíveis[56]. As diferentes características da inteligência artificial trazem distintos desafios regulatórios que se refletem também nos diferentes regimes de responsabilização[57].

Já no PL nº 2338/2023, optou-se, no artigo 27, por um regime que abranja o fornecedor e o operador de sistema de IA, determinando que, sempre que algum desses agentes causar dano patrimonial, moral, individual ou coletivo, será obrigado a repará-lo integralmente, independentemente do grau de autonomia do sistema[58].

Em continuidade, estipulou-se uma diferenciação no capítulo da responsabilidade civil: quando se tratar de sistema de IA de **alto risco ou de risco excessivo**, o fornecedor ou operador **respondem objetivamente** pelos danos causados, na

55 Código Civil, art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo. Parágrafo único. Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem.

56 LABORATÓRIO DE POLÍTICAS PÚBLICAS E INTERNET - LAPIN. **Nota técnica ao substitutivo ao PL 21/2020**. Disponível em: https://lapin.org.br/wp-content/uploads/2021/09/notatecnica-ia-pl.pdf. p. 35. Acesso em: 01 jul. 2023.

57 idem.

58 Art. 27. O fornecedor ou operador de sistema de inteligência artificial que cause dano patrimonial, moral, individual ou coletivo é obrigado a repará-lo integralmente, independentemente do grau de autonomia do sistema.

medida da participação de cada um no dano, ao passo em que, **tratando-se de IA que não seja de alto risco**, a culpa do agente causador do dano será **presumida**, aplicando-se a inversão do ônus da prova em favor da vítima[59].

A previsão é semelhante à proposta trazida na **Resolução do Parlamento Europeu** de 3 de maio de 2022 sobre a inteligência artificial na era digital, que salienta que

> *embora os sistemas de IA de alto risco devam ser abrangidos pela legislação em matéria de responsabilidade objetiva, a que se deve juntar um seguro obrigatório, todas as outras atividades, dispositivos ou processos baseados em sistemas de IA que causem danos ou prejuízos devem continuar a estar sujeitos à responsabilidade culposa; considera que as pessoas afetadas devem, contudo, beneficiar da presunção de culpa por parte do operador, a menos que este seja capaz de provar que respeitou o seu dever de diligência*[60].

A modalidade de culpa presumida é um estágio intermediário em que a culpa mantém a sua condição de requisito indispensável para a configuração do dever de indenizar, gozando, no entanto, da inversão do ônus da prova, de modo que a responsabilidade será afastada se o ofensor comprovar que não agiu com imprudência, negligência ou imperícia.

Nesse contexto, verifica-se que **há um avanço na previsão do PL nº 2338/2023 em relação à norma anterior**, eis que traz uma gradação de responsabilidade que varia com a classificação do risco, afastando a incidência absoluta da responsabilidade subjetiva.

Contudo, de nítida inspiração europeia, **compete refletir se a importação, nesse caso, é compatível e adequada com a realidade brasileira**. Ao estipular a culpa presumida para os danos causados para sistemas que não sejam caracterizados como alto risco, o PL culmina por determinar que a regra geral será a responsabilidade subjetiva, relegando as hipóteses de responsabilidade objetiva para situações excepcionais de risco alto ou excessivo.

Retorna-se, portanto, ao ponto inicial de discussão sobre a determinação apriorística de uma responsabilidade subjetiva para regimes de IA, que enfrenta

---

59 PL 2338/2023, art. 27, § 1º Quando se tratar de sistema de inteligência artificial de alto risco ou de risco excessivo, o fornecedor ou operador respondem objetivamente pelos danos causados, na medida de sua participação no dano. § 2º Quando não se tratar de sistema de inteligência artificial de alto risco, a culpa do agente causador do dano será presumida, aplicando-se a inversão do ônus da prova em favor da vítima.

60 UNIÃO EUROPEIA. **Resolução do Parlamento Europeu de 3 de maio de 2022 sobre a inteligência artificial na era digital**. Disponível em: https://www.europarl.europa.eu/doceo/document/TA-9-2022-0140_PT.html. Acesso em: 03 jul. 2023.

diversas dificuldades, especialmente no que tange à complexidade da cadeia de produção, à verificação da culpa e do causador e à determinação de quais sistemas serão considerados de alto ou baixo risco[61].

Questiona-se, ainda, a efetiva pertinência de uma alteração legislativa nesse teor no campo da responsabilidade civil, considerando a cláusula geral do risco existente no ordenamento jurídico brasileiro, a escassa maturação do debate e a fragilização da reparação integral da vítima com a centralização de uma responsabilidade subjetiva, ainda que acompanhada da presunção de culpa.

Ademais, quando se determina que os fornecedores ou operadores responderão objetivamente pelos danos causados na medida da participação de cada um no dano, o texto parece indiciar obstáculo no acesso à justiça pela vítima, eis que a averiguação da participação de cada agente no dano é especialmente complexa em cadeias de produção de sistemas de inteligência artificial[62].

61 BUARQUE, Gabriela. O Novo Marco Legal da Inteligência Artificial no Brasil e os rumos da responsabilidade civil. **Coluna Fórum de Direito Civil**. Disponível em: https://www.editoraforum.com.br/noticias/o-novo-marco-legal-da-inteligencia-artificial-no-brasil-e-os-rumos-da-responsabilidade-civil/. Acesso em: 29 jun. 2023.

62 BUARQUE, Gabriela. O Novo Marco Legal da Inteligência Artificial no Brasil e os rumos da responsabilidade civil. **Coluna Fórum de Direito Civil**. Disponível em: https://www.editoraforum.com.br/noticias/o-novo-marco-legal-da-inteligencia-artificial-no-brasil-e-os-rumos-da-responsabilidade-civil/. Acesso em: 29 jun. 2023.

10 CONCLUSÃO

O PL nº 2338/2023 representa um avanço inegável no debate regulatório sobre sistemas de IA no Brasil. Ainda que marcada por limitações dada sua falta de representatividade regional e diversidade racial, a instauração da Comissão de Juristas no Senado Federal foi fundamental para a condução de um debate técnico que levasse ao desenvolvimento de um texto que superasse o conteúdo principiológico aprovado na Câmara dos Deputados, o PL nº 21-A/2020.

Apesar disso, ressaltamos ao longo do texto pontos de melhoria, sem prejuízo de outros que possam futuramente surgir. Em primeiro lugar, tratamos sobre o **banimento de tecnologias de reconhecimento facial, policiamento preditivo, armas autônomas e de sistemas para reconhecimento de emoções**. Isso é fundamental para impedir um aprofundamento ainda maior do racismo no Brasil, especialmente no âmbito do sistema penal, bem como violações excessivas de privacidade.

Também trouxemos recomendações para aprimorar as definições apresentadas no artigo 4º, para além da inclusão do conceito de "ciclo de vida", de modo a diferenciar não fornecedores de operadores, mas sim desenvolvedores de fornecedores e aplicadores, termos mais adequados ao ecossistema de desenvolvimento da IA.

Os direitos, que são altamente bem-vindos, principalmente por sua capacidade de abarcar não só sistemas de alto risco, mas qualquer sistema, também podem ser aprimorados. Para tanto, sugerimos a ampliação de direitos de transparência e obtenção de informações. Ainda sobre transparência, defendemos a inclusão de regras para provimento de informação sobre impactos ambientais de sistemas de IA e a ampliação dos poderes da autoridade competente — que, defendemos, deve ter natureza autárquica — para incluir a prerrogativa de conduzir auditorias e de credenciar centros de pesquisa e entidades da sociedade civil para participarem da supervisão desses sistemas.

Por fim, chamamos atenção aos riscos particulares de sistemas de IA generativa e quais regras especiais devem incidir sobre elas, bem como tratamos sobre as potencialidades e as dificuldades das previsões da responsabilidade civil.

Isto posto, a Coalizão Direitos na Rede coloca-se à disposição de congressistas para apoiar seu trabalho com vistas à aprovação de uma regulação para a IA que seja protetiva de direitos e garanta, ao mesmo tempo, uma agenda de desenvolvimento que torne o Brasil um líder em IA responsável.




www.direitosnarede.org.br