Comitê Gestor da Internet no Brasil

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.cgi.br

NOTA TÉCNICA DE CONTRIBUIÇÕES DO CGI.BR AO PL 2.338/2023 – REGULAÇÃO DA INTELIGÊNCIA ARTIFICIAL NO BRASIL

INTRODUÇÃO

A regulação de sistemas de Inteligência Artificial (IA) no Brasil tem como principal proposta legislativa o PL 2.338/2023, que, após um longo processo de debate público nos últimos anos, foi aprovado pelo Senado e segue em trâmite na Câmara dos Deputados. O PL possui relevância crucial para debates acerca da inovação tecnológica e científica do país, bem como para o estabelecimento de direitos e deveres vinculados a toda cadeia de desenvolvimento, implementação e uso de sistemas de IA.

Dessa forma, o Comitê Gestor da Internet no Brasil (CGI.br) vem se posicionando e contribuindo com o debate público acerca da regulação da IA, valendo-se de sua natureza multissetorial para a promoção de diálogos e recomendações que considerem a relevância da IA para o desenvolvimento socioeconômico do país, sem olvidar a indispensável proteção de direitos fundamentais de pessoas e grupos afetados.

Em Nota Pública de 14 de novembro de 2025[1], **o CGI.br reforçou a importância de manter e fortificar as classificações de riscos e deveres presentes no projeto, assim como os mecanismos de transparência e explicabilidade** que colaboram para a identificação e mitigação de vieses e discriminações que podem ocorrer em sistemas de IA.

Por sua vez, em Nota Técnica sobre o PL 6.237/2025[2], o Comitê manifestou-se sobre o sistema de governança e os arranjos institucionais acerca da regulação da inteligência artificial no país, enfatizando sua disponibilidade e competência técnica para integrar o ecossistema regulatório de IA e, em específico, o Comitê de Regulação e Inovação em Inteligência Artificial – CRIA.

Ademais, o CGI.br solicitou em Nota Pública[3] que a Câmara dos Deputados garanta tempo adequado entre a apresentação do substitutivo do PL 2.338/2023 do Relator na Comissão Especial responsável e a votação final em Plenário. Com essa solicitação, o Comitê endossa a relevância em promover procedimentos inclusivos e transparentes, que permitam fluxos e prazos razoáveis para que os di-

[2] COMITÊ GESTOR DA INTERNET NO BRASIL. Nota Técnica sobre o PL 6.237/2025. Disponível em: https://cgi.br/publicacao/nota-tecnica-do-cgi-br-sobre-o-pl-6-237-2025-governanca-de-inteligencia-artificial/

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.cgi.br

ferentes setores da sociedade possam tomar conhecimento sobre as propostas e participar de maneira qualificada nos processos de tomada de decisão em torno da regulação de sistemas de IA no Brasil.

Assim, após um período de análise e diálogo multissetorial, o CGI.br elaborou a presente Nota Técnica com o objetivo de avançar em suas contribuições sobre o PL 2.338/2023, fornecendo recomendações mais específicas sobre possibilidades de melhorias no texto do PL, além de avaliações sobre aspectos gerais que possam contribuir para discussões importantes ainda em aberto pelos mais variados atores interessados nesse processo regulatório.

1. **A IMPORTÂNCIA DO PL 2.338/2023**

O PL 2.338/2023 representa um avanço no debate regulatório sobre sistema de IA no Brasil, buscando, equilibrar, de um lado, a proteção de direitos fundamentais e a mitigação dos riscos conhecidamente oferecidos por esses sistemas e, de outro, preservar a inovação e o desenvolvimento tecnológico no país, por meio de uma regulação assimétrica e uma abordagem baseada em riscos.

O texto do PL 2.338/2023 estabelece obrigações, instrumentos de governança e um arranjo fiscalizatório que contribui para operacionalizar o exercício desses direitos, assim como define usos inaceitáveis de IA e cria medidas de governança específicas que devem ser adotadas em relação a sistemas de alto risco e àquelas que forem adotadas pelo setor público.

Dessa forma, o PL acertadamente estabelece uma regulação assimétrica e baseada em riscos, direcionando uma carga regulatória mais intensa quanto maior for o grau de risco do sistema, que terá, assim, mais deveres de governança. De forma prática, a IA que não for classificada como de alto risco e tampouco IA generativa ou de propósito geral possui poucas e menos complexas obrigações, devendo apenas prover informações sobre a interação com seu sistema, garantir o direito à proteção de dados e à não discriminação — direitos, inclusive, já previstos em outras legislações. Para além dessa divisão de risco excessivo e alto risco, o texto do projeto, em diversos momentos, reforça a necessidade de autoridade competente ou setorial estabelecer obrigações simplificadas para empresas de pequeno porte, startups e instituições de pesquisa mesmo que desenvolvam, apliquem ou distribuam IAs de alto risco[4]. Nesse sentido, **o CGI.br reforça que uma regulação proporcional e assimétrica é essencial para a atribuição de deveres e responsabilidades que não impeçam o desenvolvimento tecnológico e a inovação**, como já mencionado em Nota Pública[5].

[4] O texto atual do PL, por exemplo, prevê que a autoridade setorial estabeleça prazos especiais e procedimentos simplificados para o exercício do direito à explicação de acordo com o porte do operador (Art. 7º); devem também definir critérios diferenciados para sistemas de IA ofertados por microempresas, empresas de pequeno porte e startups que promovam o desenvolvimento da indústria tecnológica nacional (Art. 67); assim como o SIA deve regulamentar regimes simplificados para casos de pesquisa científica e tecnológica no ambiente produtivo com vistas ao alcance da autonomia tecnológica, ou projetos de interesse público, dentre outras situações (Art. 73).

[5] Cf. https://cgi.br/esclarecimento/nota-publica-sobre-pl-2-338-2023-e-regulacao-de-sistemas-de-ia-no-brasil/.

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.cgi.br

Ademais, o CGI.br saúda que o atual texto do PL estabelece mecanismos de fomento ao setor produtivo, como o incentivo a compras públicas de sistemas de IA nacionais e o desenvolvimento de ambientes de experimentação tecnológica para atores de diferentes portes. O Comitê também destaca a relevância de uma proposta de arquitetura regulatória policêntrica e descentralizada, atenta às especificidades setoriais, assim como a relevância da indicação da Agência Nacional de Proteção de Dados (ANPD) como coordenadora do Sistema Nacional de Regulação e Governança de Inteligência Artificial (SIA).

Adicionalmente, sobre os avanços do PL 2.338/2023, o Comitê reforça a relevância da seção IV do PL, que versa sobre os direitos de autor e conexos. Ainda que essa matéria possa ter especificações regulatórias mais detalhadas futuramente, é imprescindível que um marco legal de IA não se abstenha de definir uma base para garantia de direitos e disposições de deveres relacionados aos impactos de sistemas de IA sobre direitos autorais.

Por fim, o CGI.br reafirma a importância da manutenção de um texto legal focado na proteção da pessoa humana e de seus direitos fundamentais. O PL 2.338/2023 avançou expressivamente ao prever entre seus fundamentos, no Art. 2º, V, a igualdade, a não discriminação, a pluralidade e a diversidade. Além disso, entre os princípios e as definições previstos está a não discriminação ilícita ou abusiva. Essas disposições são ainda fortalecidas pela inclusão da discriminação indireta, disposição fundamental considerando o funcionamento e impactos não previstos de sistemas de IA.

2. RECOMENDAÇÕES DO CGI.BR PARA APRIMORAMENTO DO PL 2.338/2023

2.1. CATEGORIZAÇÃO DE RISCO: ALTO, EXCESSIVO E ANÁLISE DE RISCO

O PL 2.338/2023 adota, em grande medida, uma abordagem regulatória baseada em riscos. No entanto, o desenho regulatório adotado pelo texto legislativo carece de algum delineamento para evitar equívocos e contradições na sua interpretação. Exemplo disso é que uma proposta regulatória baseada essencialmente na identificação e avaliação do risco e, se necessário, adoção de medidas para mitigá-lo, torne, de forma contraditória, a análise do risco pelo regulado **opcional** — como faz a atual redação do Art. 12[6].

Há diversas concepções sobre o que é risco, mas, de maneira geral, pode ser entendido como externalidades negativas que podem ocorrer em um futuro incerto e resultar em danos individuais e coletivos; pode ser entendido, também, como o produto da probabilidade da ocorrência de um evento e suas consequências, que dizem respeito a eventos que causem ameaça a algo de valor

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

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.cgi.br

humano[7]. Ao longo do tempo, a concepção sobre risco se transformou e se torna objeto de governança pública, em que o poder público cria formas para coletar dados, determinar níveis toleráveis de riscos e gerenciá-los por meio da regulação, buscando controlar, assim, potenciais consequências adversas[8].

Desse modo, em suma, a regulação de risco busca a adoção de medidas que gerenciam riscos decorrentes de certas atividades. O PL 2.338/2023 pode ser entendido não apenas como uma regulação de risco (como são tantas outras), mas como uma *regulação baseada em risco*, uma abordagem regulatória que considera as **perspectivas do regulador e do regulado**. De um lado, prescreve que a atuação do regulador priorize os riscos decorrentes da inação ou ação perante setores e agentes regulados, a partir de uma metodologia interna de levantamento e mensuração e, de outro, pode ditar ao agente regulado **a adoção de mecanismos e instrumentos internos de avaliação e gerenciamento de riscos**[9].

Tal mudança no foco regulatório integra um contexto maior de crise do modelo regulatório durante as décadas de 1980 e 1990, em que um modelo mais prescritivo passou a ser visto como um obstáculo ao desenvolvimento econômico, de alto custo e ineficiente[10]. Em outras palavras, a presente abordagem transfere (e prescreve) aos entes regulados parte dos custos regulatórios por meio da adoção de mecanismos de autoavaliação e gerenciamento de riscos pelos próprios regulados.

Não se busca aqui fazer uma avaliação de modelos regulatórios, mas **explicitar que se trata de um modelo que transfere a alocação e o gerenciamento de riscos do Estado aos entes privados, de forma que se torna contraditório transferir e, ao mesmo tempo, desobrigar os entes privados a realizarem a avaliação dos riscos de suas atividades, como faz o Art. 12** do PL 2.338/2023.

A análise de risco prévia é estabelecida como mera possibilidade aos entes regulados, quando é base para a categorização do risco da atividade e sua consequente (i)legalidade (definição como risco excessivo ou não) e definição de mecanismos de gestão de risco, isto é, necessidade, ou não, de observar as medidas e obrigações estabelecidas para sistemas de IA de alto risco. Em outras palavras, uma **análise prévia de risco é peça-chave para a compreensão e observância da legislação como um todo**, de forma que a sua realização deve ser uma obrigação geral para que os entes

[7] Cf. KAPLAN, S.; GARRICK, J. On the quantitative definition of risk. Risk Analysis, 1(1), 11-27, 1981.; FISHER, Elizabeth. Risk regulatory concepts and the law. In: *OCDE*, Risk and regulatory Policy: Improving the Governance of Risk. Relatório, 2010; ARAUJO, Heloisa Bianquini. *Proteção de dados pessoais e regulação baseada em risco*: construção institucional da regulamentação pela Autoridade Nacional de Proteção de Dados. 2024. 272 f. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2024..

[8] ALEMANNO, A. Risk and regulation. In: BURGESS, A.; ALEMANNO, O.; ZINN, J. O. (Eds.). *Routledge Handbook of Risk Studies*, p. 191-203. Londres: Routledge, 2016; HUBER, M. Colonised by risk – the emergence of academic risks in British higher education. In: HUTTER, B. M. (Ed.). *Anticipating risks and organizing risk regulation*, p. 114-135. Cambridge: Cambridge University Press, 2010. apud ARAUJO, 2024.

[9] BLACK, Julia. Risk-based regulation: choices, practices and lessons being learnt. In: *OECD*. Risk and Regulatory Policy. OECD Reviews of Regulatory Reform, OECD Publishing, Paris, 2010.

[10] MACENAITE, Milda. *The "riskification" of European Data Protection Law through a two-fold shift*. European Journal of Risk Regulation, v. 8, n. 3, p. 506-540, 2017.

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.cgi.br

regulados possam ter instrumentos para identificar corretamente o enquadramento do seu sistema de IA.

Ademais, uma análise prévia de IA não precisa (e não deve) ser um instrumento complexo e extenso como é, por exemplo, uma Avaliação de Impacto Algorítmico (AIA)[11] — que possui metodologias e requisitos específicos —, mas pode ser um simples estágio no desenvolvimento de uma IA, em que se observam os parâmetros legais e regulatórios para sistemas de IA de alto risco ou de risco excessivo e os compara com as atividades desenvolvidas pelo ente regulado, podendo tomar como base modelos estabelecidos pela autoridade competente ou setorial.

Assim, a fim de evitar que obrigações essenciais para a proteção de direitos fundamentais não sejam observadas em virtude da ausência de uma análise preliminar de risco, **recomenda-se que a análise preliminar de risco seja um dever estabelecido pelo PL** de forma proporcional ao porte e impacto potencial do sistema de IA, devendo ser simplificado em casos específicos na regulamentação, especialmente para micro, pequenas e médias empresas e para sistemas de baixo impacto sobre direitos fundamentais.

Art. 12. Antes de sua introdução e circulação no mercado, emprego ou utilização, o agente de IA ~~poderá~~ **deverá** realizar avaliação preliminar para determinar o grau de risco do sistema, baseando-se nos critérios previstos neste Capítulo, de acordo com o estado da arte do desenvolvimento tecnológico. ~~§ 1º A realização da avaliação preliminar será considerada como medida de boa prática e poderá resultar em benefícios para o agente de IA para fins do disposto no art. 50, § 1º, podendo, inclusive, receber tratamento prioritário em procedimentos para avaliação de conformidade, nos termos do art. 34, ambos desta Lei~~. § 1º Caberá à autoridade setorial, ou ao regulador residual, definir as hipóteses em que a avaliação preliminar poderá ser simplificada, observados critérios técnicos e o interesse público.

Reforça-se ainda a importância de o texto do PL prever a possibilidade da **identificação de novas hipóteses de alto risco**, via regulamentação e processo que garanta participação social e de análise de impacto regulatório, observados critérios objetivos, parâmetros previamente definidos em lei e vedada a ampliação automática ou indeterminada de hipóteses sem fundamentação técnica expressa, considerando a probabilidade e a gravidade dos impactos adversos sobre pessoas ou grupos afetados e outros critérios definidos em lei (Art. 15 e 16).

[11] Na Avaliação de Impacto dos Sistemas de IA na regulação europeia, por exemplo, os responsáveis pela implantação de uma IA de risco elevado devem cumprir uma série de requisitos, como: uma descrição dos processos em que o sistema de IA de risco elevado seja utilizado de acordo com a sua finalidade prevista; uma descrição do período em que o sistema se destina a ser utilizado e com que frequência; as categorias de pessoas singulares e grupos suscetíveis de serem afetados; uma descrição da aplicação das medidas de supervisão humana; as medidas a tomar caso esses riscos se materializem, dentre outros (Artigo 27.o, do Regulamento UE 2024/1689). Ao passo que, "Um prestador que considere que um dos sistemas de IA a que se refere o anexo III [sobre Sistemas de IA de risco elevado] não é de risco elevado deve **documentar a sua avaliação antes de esse sistema ser colocado no mercado ou colocado em serviço** (Art. 6.o, 4)", isto é, sem requisitos e etapas técnicas a serem cumpridas, para além de documentar a justificativa, registar-se e registar esse sistema na base de dados da UE relativa a sistemas de IA de risco elevado.

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.cgi.br

A manutenção desse rol de hipóteses como exemplificativo é importante para garantir a possibilidade do processo regulatório observar atenta e tempestivamente o desenvolvimento, a implementação e a utilização de sistemas de IA de alto risco que ainda não foram tratados objetivamente pelo PL, desde que assegurada previsibilidade regulatória e prazo razoável de adaptação para os agentes econômicos impactados.

Um exemplo disso são os sistemas de IA que podem impactar o direito fundamental à liberdade de expressão, como aqueles que atuam na moderação de conteúdo online, que podem causar inúmeros danos coletivos e individuais, mas que na proposta atual não teriam aplicação da legislação de inteligência artificial, sendo necessária a criação de legislação específica nos termos do Art. 77 do PL 2.338/2023. Nesse sentido, o CGI.br acentua **a importância de retirar integralmente o Art. 77 para permitir que essa matéria seja devidamente apreciada em processo regulatório**, tendo em vista seus expressivos impactos para direitos de pessoas afetadas por esses sistemas de IA, ressalvada a necessidade de coordenação normativa com o Marco Civil da Internet e eventual legislação específica sobre plataformas digitais a fim de evitar sobreposição regulatória. Em outras palavras, impedir que o regulador possa atuar em sistemas de IA que firam a liberdade de expressão, entre eles sistemas de moderação de conteúdo, é incongruente com os próprios fundamentos e princípios do texto de lei proposto.

Desse modo, destaca-se o quanto esses arranjos de reclassificação contínua dos sistemas de IA garantem o estabelecimento de uma legislação tecnologicamente neutra — isto é, que permita a aplicação sobre tecnologias futuras — e estabelecem um arranjo institucional participativo e colaborativo, em que empresas, especialistas e entidades interessadas podem contribuir com a reclassificação de riscos, assim como estabelecem instrumentos de prestação de contas por meio da análise de impacto regulatório.

2.1.1. Uso de sistemas de IA para abuso e exploração sexual como risco excessivo e necessidade de abordagem mais ampla sobre deepfakes

Um dos aspectos centrais, no texto do PL 2.338/2023, é o estabelecimento de um rol de usos e aplicações de IA inaceitáveis, definidas como riscos excessivos e dispostas no artigo 13. Um exemplo da relevância de se identificar situações e riscos inaceitáveis é a vedação de sistemas que tenham o propósito de "d) possibilitar a produção ou disseminação ou facilitar a criação de material que caracterize ou represente **abuso sexual ou exploração sexual de crianças e adolescentes**" (grifo nosso).

O trecho é especialmente relevante, considerando o aumento expressivo na circulação de deepfakes sexuais em escolas do país. Em 2025, a Safernet Brasil publicou um mapeamento que identificou 16 casos envolvendo 72 vítimas, distribuídos em 10 estados brasileiros. De forma mais ampla, 90% do público composto por crianças e adolescentes entre 9 e 17 anos de idade é usuário de Internet

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.cgi.br

no Brasil[12], enquanto, no mundo, o grupo representa 1/3 de todos os usuários de Internet[13]. Trata-se de um segmento hipervulnerável em período de desenvolvimento biopsicossocial, como apontado por pesquisadoras do Instituto Alana[14], e reconhecido pelo PL 2.338/2023 em seu artigo 4º, XVII.

Contudo, nesse mesmo contexto, **observa-se que o PL não possui nenhuma alínea dedicada ao segmento mais impactado pelas deepfakes sexuais: mulheres**. Mais de 90% dos alvos das deepfakes sexuais são mulheres, de acordo com o estudo *Deepfake Abuse: Landscape Analysis*[15]. Nesse sentido, recomenda-se que o escopo de aplicação do rol de riscos excessivos seja amplificado para incorporar tais casos.

Uma sugestão de redação possível é incluir uma alínea adicional propondo a **vedação** de conteúdo sintético que:

> Art. 13. São **vedados** o desenvolvimento, a implementação e o uso de sistemas de IA:
>
> I - com o propósito de: [...]
>
> e) possibilitar a produção ou disseminação ou facilitar a criação de material que caracterize ou represente cena de nudez ou conteúdo sexual **sem o consentimento expresso** das pessoas retratadas;

Dessa forma, não somente seriam incluídas no escopo de proteção as mulheres, mas também quaisquer grupos que sejam vitimizados por este tipo de violência sexual online. É importante reforçar que se considera como conteúdo sexual tanto aquele de natureza explícita como aquele implícito, manipulado ou sugestivo.

Além disso, destaca-se a necessidade de uma especificação sobre o uso de deepfakes em contextos mais gerais, que também causam danos coletivos e individuais. As deepfakes estão no cerne de diversas práticas de natureza desinformativa, produzindo efeitos políticos graves e violações de conteúdo moral. O texto do PL 2.338/2023 não abarca essas situações, sendo importante considerar a

[12] NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR – NIC.br; CENTRO REGIONAL DE ESTUDOS PARA O DESENVOLVIMENTO DA SOCIEDADE DA INFORMAÇÃO – CETIC.br. *Pesquisa sobre o uso da Internet por crianças e adolescentes no Brasil*: TIC Kids Online Brasil 2023 (relatório completo). São Paulo: NIC.br/Cetic.br, 13 set. 2024. Disponível em: https://cetic.br/media/analises/tic_kids_online_brasil_2023_principais_resultados.pdf

[13] UNICEF – United Nations Children's Fund. *The State of the World's Children 2017*: Children in a Digital World. New York: UNICEF, 2017. Disponível em: https://www.unicef.org/reports/state-worlds-children-2017

[14] HENRIQUES, Isabella; MACIEL, Emanuella Ribeiro Halfeld. Como o PL da IA aborda a proteção integral de crianças e adolescentes? *JOTA*, 26 jun. 2024. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/ia-regulacao-democracia/como-o-pl-da-ia-aborda-a-protecao-integral-de-criancas-e-adolescentes

[15] My Image, My Choice (2024) *Deepfake Abuse Landscape Analysis*: The exponential rise of deepfake abuse in 2023-2024. Disponível em: https://www.canva.com/design/DAGLHpt6WlY/Hfztqtw_-tKza_2l1cPNrA/view?utm_content=DAGLHpt6WlY&utm_campaign=designshare&utm_medium=link&utm_source=editor

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.cgi.br

possibilidade de incluir um inciso que especifique esse potencial uso inadequado na listagem de sistemas de IA de alto risco.

Cabe ainda destacar que o texto do PL prevê a definição de conteúdo sintético[16] e a necessidade de sua sinalização (Art. 19). No entanto, de um lado, sua exigência está atrelada a sistemas de alto risco — o que exclui uma série de agentes e situações relevantes — e, de outro, o conceito de deepfake se distingue, em alguma medida, da definição de conteúdo sintético — podendo exigir regramentos diferenciados e mais estritos.

2.1.2. Impactos da não adoção de medidas para coibir efeitos ilícitos (risco excessivo)

No artigo 13, que trata de risco excessivo, consta que "são vedados o desenvolvimento, a implementação e o uso de sistemas de IA **'com o propósito de'**" — ao qual se segue uma lista de hipóteses, a saber:

> a) instigar ou induzir o comportamento da pessoa natural ou de grupos de maneira que cause danos à saúde, à segurança ou a outros direitos fundamentais próprios ou de terceiros;
> b) explorar quaisquer vulnerabilidades da pessoa natural ou de grupos com o objetivo ou o efeito de induzir o seu comportamento de maneira que cause danos à saúde, à segurança ou a outros a direitos fundamentais próprios ou de terceiros;
> c) avaliar os traços de personalidade, as características ou o comportamento passado, criminal ou não, de pessoas singulares ou grupos, para avaliação de risco de cometimento de crimes, de infrações ou de reincidência;
> d) possibilitar a produção ou disseminação ou facilitar a criação de material que caracterize ou represente abuso ou exploração sexual de crianças e adolescentes;

Reconhecendo que mesmo sistemas de Inteligência Artificial com propósitos legítimos podem sistematicamente ocasionar os efeitos descritos nas alíneas a-d e que identificar a intencionalidade de sistemas de IA pode ser desafiador, o texto do PL prevê, no mesmo artigo, que os "desenvolvedores de sistemas de IA devem adotar medidas para coibir o uso de seus sistemas para as hipóteses descritas no caput inciso I deste artigo" (§ 1º).

Um exemplo da limitação em potencial desta formulação seria o caso da IA generativa Grok, sob acusação, recentemente, de violar os direitos de crianças, adolescentes e mulheres[17] ao gerar imagens de abuso não consentidas em larga escala através de uma de suas funcionalidades[18]. No site

---

16 "Art. 4º. [...] XXI – conteúdos sintéticos: informações, tais como imagens, vídeos, áudio e texto, que foram significativamente modificadas ou geradas por sistemas de IA;"

17 IDEC - Instituto de Defesa do Consumidor. Idec pede ao governo suspensão da IA "Grok" por violações de direitos de crianças, adolescentes e mulheres. Publicado em 12/01/2026. Acesso em 14/01/2026. Disponível em: https://idec.org.br/release/idec-pede-ao-governo-suspensao-da-ia-grok-por-violacoes-de-direitos-de-criancas-adolescentes. Acesso em: 13/01/2026.

18 HELDER, Darlan. 'Sentimento horrível. Me sinto suja', diz brasileira vítima de foto editada de biquíni pelo Grok, IA de Musk. *G1* (online). Publicado em 08/01/2026. Acesso em 14/01/2026. Disponível em:

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 5509 3511
fax: 55 11 5509 3512
www.cgi.br

da empresa, a Grok é apresentada como um assistente de IA "em busca da verdade, oferecendo respostas diretas e sem filtros, com recursos avançados de raciocínio, programação e processamento visual"[19] (tradução livre). É possível afirmar que o assistente não foi desenhado com o intuito de produzir essas imagens de abuso — ficando, portanto, fora do escopo de usos vedados pela redação atual —, mas também é certo que produziu esta consequência sobre os grupos afetados, devendo ser responsabilizado pelos efeitos sistêmicos ocasionados em decorrência do desenho permissivo da IA.

A fim de evitar que casos como este — em que a análise de intencionalidade pode implicar uma barreira à proteção de direitos —, considera-se que o § 1º pode ser aprimorado para prever a possibilidade de que sistemas de IA que reiterada e comprovadamente não coíbam o uso de seus sistemas para as hipóteses descritas no inciso I sejam classificadas como de risco excessivo, após processo fiscalizatório ou sancionatório conduzido por autoridade competente.

Art. 13. São vedados o desenvolvimento, a implementação e o uso de sistemas de IA: I – com o propósito de: [...] § 1º Os desenvolvedores de sistemas de IA devem adotar medidas para coibir o uso de seus sistemas para as hipóteses descritas no ~~caput~~ inciso I[20] deste artigo, sendo que a não adoção reiterada, comprovada em processo fiscalizatório ou sancionatório conduzido pela autoridade setorial ou regulador residual, pode implicar na classificação do sistema de IA como de risco excessivo e em sua consequente vedação.

2.1.3. O PL permite uso amplo e irrestrito de sistemas de identificação biométrica à distância e em tempo real

O artigo 13, apesar de inicialmente vedar sistemas de identificação biométrica à distância, em tempo real e em espaços acessíveis ao público, cria um amplo conjunto de **exceções** que, na prática, podem gerar um vácuo regulatório acerca dos principais usos destas tecnologias no contexto da segurança pública no país.

Isso porque, além da amplitude das exceções, o funcionamento desses sistemas, a exemplo do reconhecimento facial à distância em tempo real, não pode ser considerado como "de uso pontual", sendo, portanto, incompatível com as restrições propostas[21]. Tais tecnologias, para identificar uma

https://g1.globo.com/tecnologia/noticia/2026/01/08/sentimento-horrivel-me-sinto-suja-diz-brasileira-vitima-de-foto-editada-de-biquini-pelo-grok-ia-de-musk.ghtml. Acesso em: 13/01/2025.

[19] "Grok is your truth-seeking AI companion for unfiltered answers with advanced capabilities in reasoning, coding, and visual processing." Disponível em: https://x.ai/grok. Acesso em 13/01/2026.

[20] Entende-se que a remissão ao caput é um erro redacional, já que não há descrição de hipóteses de usos de IA no caput, mas no inciso I.

[21] O uso de tecnologias de reconhecimento facial a distância e em tempo real é permitido para as seguintes hipóteses, segundo o Art. 13: "a) instrução de inquérito ou processo criminal, mediante autorização judicial prévia e motivada,

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.cgi.br

determinada pessoa procurada pela justiça, desaparecida, ou por qualquer outro motivo, dependem de uma captura constante de dados sensíveis biométricos, isto é, do monitoramento de toda e qualquer pessoa que passa na área monitorada. De acordo com dados de dezembro de 2025 do projeto "O Panóptico" gerido pelo Centro de Estudos de Segurança e Cidadania (CESeC), existem 495 projetos ativos que utilizam técnicas de reconhecimento facial em segurança pública no Brasil, totalizando 87.154.023 pessoas potencialmente vigiadas por reconhecimento facial no país[22].

Na prática, isso significa que uma câmera de reconhecimento facial não seria "ligada e desligada" para investigar a autoria de uma infração penal após decisão judicial — até porque, após a decisão judicial, o fato já ocorreu, de forma que o sistema de reconhecimento facial já precisaria estar previamente ativado —; muito menos para detectar um flagrante delito — já que isso incluiria prever quando um crime irá ocorrer para, então, detectá-lo. Em resumo, as hipóteses de uso listadas, como busca de pessoas desaparecidas ou flagrante delito de crimes, somente podem ocorrer se o monitoramento estiver prévia e constantemente em curso.

Ademais, tais situações, excetuadas do Art. 13, não são explicitamente inseridas como de alto risco, fazendo com que sistemas de IA de conhecido alto impacto corram o risco de ficar de fora das principais obrigações estabelecidas no projeto.

Ainda que se considerasse que as finalidades excetuadas no Art. 13 são específicas, são diversos os casos que ilustram o uso dessas tecnologias para finalidades diversas e ilegais. O Sistema de Reconhecimento Facial para Fugitivos (SRFP) implementado na Cidade de Buenos Aires para buscar cerca de 40 mil fugitivos foi usado para obter informações pessoais de cerca de 10 milhões de pessoas[23]. Os abusos do programa de vigilância Cortex[24] [25] também ilustram bem como instrumentos de vigilância em escala são comumente utilizados de forma ilegítima.

Os usos previstos dos sistemas identificação biométrica à distância também contrariam **princípios da Administração Pública** – como legalidade, economicidade, publicidade e eficiência – considerando que esta tem o dever de demonstrar que os investimentos realizados produzem resultados

---

quando houver indícios razoáveis da autoria ou participação em infração penal, a prova não puder ser feita por outros meios disponíveis e o fato investigado não constituir infração penal de menor potencial ofensivo; b) busca de vítimas de crimes e de pessoas desaparecidas, ou em circunstâncias que envolvam ameaça grave e iminente à vida ou à integridade física de pessoas naturais; c) flagrante delito de crimes punidos com pena privativa de liberdade superior a 2 (dois) anos, com imediata comunicação à autoridade judicial; d) recaptura de réus evadidos e cumprimento de mandados de prisão e de medidas restritivas ordenadas pelo Poder Judiciário".

[22] Cf: https://www.opanoptico.com.br/#regioes

[23] CONVERGÊNCIA DIGITAL. Justiça argentina proíbe reconhecimento facial após prisões indevidas. *Convergência Digital*, 08 set. 2022. Disponível em: https://convergenciadigital.com.br/seguranca/justia-argentina-probe-reconhecimento-facial-aps-prises-indevidas/

[24] VALENTE, Rubens; FREITAS, Caio. Programa de vigilância do MJ permite a 55 mil agentes seguir "alvos" sem justificativa. *Agência Pública* (online). Publicado em 09/10/2024. Disponível em: https://apublica.org/2024/10/vigilancia-55-mil-agentes-podem-monitorar-alvos-sem-justificativa/. Acesso em 19/01/2026.

[25] SILVA, Vinicius; ZANATTA, Rafael. Por que precisamos rever o uso do Córtex no Brasil?. *Data Privacy Brasil Research* (online). Publicado em 12/12/2024. Disponível em: https://www.dataprivacybr.org/por-que-precisamos-rever-o-uso-do-cortex-no-brasil/. Acesso em: 19/01/2026.

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.cgi.br

compatíveis com os custos. Trata-se de uma tecnologia que tem sido empregada no país seguindo um padrão de investimentos maciços injustificados, baixa taxa de acertos, falta de transparência, ausência de supervisão e monitoramento, carência de evidências acerca da eficácia para os fins propostos e casos graves de danos ocasionados por detenções de inocentes quando utilizados em contexto de segurança pública, de acordo com levantamento nacional realizado pelo CESeC em parceria com a Defensoria Pública da União em 2025[26].

Além disso, os sistemas a que se referem o artigo abarcam tecnologias de reconhecimento facial, cuja baixa acurácia cria vieses raciais e de gênero, produzindo efeitos discriminatórios, em especial para pessoas e grupos vulnerabilizados, o que já está amplamente documentado pela literatura científica[27][28]. Ao permitir o monitoramento à distância, em tempo real e em espaços acessíveis ao público, abre-se espaço para o armazenamento indiscriminado de imagens e para a vigilância em larga escala. Isso afeta diretamente direitos fundamentais como o direito à **privacidade, à proteção de dados pessoais**, à **livre associação**, além de criar um efeito inibitório sobre a **liberdade de expressão e manifestação**. Também desrespeita os princípios da finalidade e da necessidade da LGPD, uma vez que a vigilância em larga escala excede o mínimo dispensável para a persecução penal[29].

Nesse sentido, por ser uma tecnologia que tem como base o tratamento de dados pessoais biométricos para entregar seus resultados, torna-se fundamental alinhar seu desenvolvimento, sua implementação e seu uso de acordo com o disposto na LGPD, o que o texto do PL não faz diretamente.

Como previsto no Art. 5º da LGPD, os dados biométricos são considerados dados sensíveis, ou seja, são dados que, se utilizados de forma indevida, podem gerar discriminação e outros graves danos aos seus titulares e seus direitos fundamentais. Dessa forma, a lei prevê um regramento mais rigoroso para o tratamento desses dados. Se consideramos ainda o contexto de uso desses dados para segurança pública, a LGPD não se aplica, mas determina em seu Art. 4º, § 1º, que esse tipo de tratamento de dados será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos na LGPD.

Sendo assim, a atual previsão do PL 2.338/2023 sobre sistemas de identificação biométrica à distância, em tempo real ignora a necessidade de uma legislação específica sobre o tratamento de

[26] NUNES, Pablo et al. *Mapeando a vigilância biométrica* [livro eletrônico]: levantamento nacional sobre o uso do reconhecimento facial na segurança pública. Rio de Janeiro: CESeC, 2025. Disponível em: https://drive.google.com/file/d/1bN2ssBp_dMiih8YOUonLhGl_5jRoNe5s/view. Acesso em 15/01/2026.
[27] BUOLAMWINI, Joy; GEBRU, Timnit. Gender shades: Intersectional accuracy disparities in commercial gender classification. In: *Conference on fairness, accountability and transparency*. PMLR, 2018. p. 77-91.
[28] 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 15/01/2026.
[29] COALIZÃO DIREITOS NA REDE. Projeto de Lei nº 2.338/2023 (Nota Técnica). *Coalizão Direitos na Rede*, agosto, 2023. Disponível em: https://direitosnarede.org.br/wp-content/uploads/2023/08/Nota-tecnica-PL-que-regula-a-IA.pdf. Acesso em 15/01/2026.

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.cgi.br

dados pessoais para fins de segurança pública ou atividades de investigação e repressão de infrações penais, ampliando desproporcionalmente as exceções para essas tecnologias, sem considerar que essa matéria ainda carece de maior detalhamento regulatório e legislativo no Brasil.

Posto isso, sugerimos que o artigo 13 seja mantido, vedando o uso de tais sistemas, mas que sejam **removidas todas as hipóteses que produzem exceções**.

Art. 13. São vedados o desenvolvimento, a implementação e o uso de sistemas de IA: [...]
IV – em sistemas de identificação biométrica à distância, em tempo real e em espaços acessíveis ao público~~, com exceção das seguintes hipóteses:~~
~~a) instrução de inquérito ou processo criminal, mediante autorização judicial prévia e motivada, quando houver indícios razoáveis da autoria ou participação em infração penal, a prova não puder ser feita por outros meios disponíveis e o fato investigado não constituir infração penal de menor potencial ofensivo; b) busca de vítimas de crimes e de pessoas desaparecidas, ou em circunstâncias que envolvam ameaça grave e iminente à vida ou à integridade física de pessoas naturais; c) flagrante delito de crimes punidos com pena privativa de liberdade superior a 2 (dois) anos, com imediata comunicação à autoridade judicial; d) recaptura de réus evadidos e cumprimento de mandados de prisão e de medidas restritivas ordenadas pelo Poder Judiciário.~~
[...]
§ 2º: Eventuais exceções ao inciso IV deste artigo podem ser estipuladas pela autoridade setorial, ou pelo regulador residual[30], estritamente para atividades de segurança pública, persecução penal e busca de pessoas desaparecidas, desde que garantido o processo regulatório com escuta pública e respeito aos direitos fundamentais, observados critérios técnicos objetivos, avaliação prévia de risco, publicidade dos parâmetros adotados e coordenação normativa nacional, de modo a evitar fragmentação regulatória.
§ 3º A possibilidade de exceções como disposta no § 2º deste artigo deverá ser regida por legislação específica, de forma a ser proporcional e estritamente necessária ao atendimento do interesse público, observados o devido processo legal e o controle judicial, bem como os princípios e direitos previstos nesta Lei e, no que couber, na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), especialmente a garantia contra a discriminação e a necessidade de revisão da inferência algorítmica pelo agente público responsável, assegurada revisão humana, com possibilidade de contestação, fundamentação individualizada da decisão e registro documentado e auditável da intervenção realizada.

2.1.4. Uso de sistemas de IA para prever crimes é discriminatório

[30] O PL 6.237/2025, proposto pelo Executivo, a fim de sanar eventual vício de iniciativa, atribui à ANPD competências de orientações normativas gerais — assim como o PL 2.338/2023 — e de regulador residual para "exercerá competência normativa, regulatória, fiscalizatória e sancionatória plena sobre o desenvolvimento, a distribuição e o uso de modelos e aplicações de inteligência artificial em atividades econômicas e sociais não submetidas a um órgão ou ente regulador setorial específico".

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 5509 3511
fax: 55 11 5509 3512
www.cgi.br

O uso de um sistema de IA para **previsão** de infrações reais ou potenciais em investigações integra o escopo do que é conhecido como policiamento preditivo. A abordagem vem sendo empregada como estratégia de prevenção de crimes e se baseia em um grande volume de dados e no uso de algoritmos complexos para predizer onde e quando pode acontecer um evento criminal[31].

Reiteramos que o uso de modelos de inteligência artificial e *big data* podem ser úteis para a produção de conhecimento em processos investigativos. No entanto, a premissa de que é possível prever tais eventos antes de uma suposta ocorrência contraria diretamente direitos fundamentais como a presunção de inocência e a igualdade perante a lei[32], sendo algo que não pode ser corrigido por meros ajustes ou melhorias técnicas e metodológicas, uma vez que se trata de algo problemático desde a concepção. Não há condições apriorísticas que tornem qualquer indivíduo criminalizável antes que a — hipotética — infração ocorra.

Em termos práticos, um efeito possível é que quaisquer grupos sociais que historicamente estiverem associados a maiores taxas de violência sejam considerados mais propensos a se envolver em crimes, incorrendo numa correlação espúria com consequências discriminatórias[33]. Em outras palavras, grupos pertencentes a determinada raça, classe e área geográfica seriam alvos preferenciais de vigilância e violência estatal, atualizando mecanismos de racismo institucional e retroalimentando ciclos de vulnerabilização[34]. Diante do exposto, no que concerne ao PL 2.338/2023, sugerimos que o inciso X do artigo 14 seja alterado, retirando a possibilidade de previsão da ocorrência ou recorrência de infração com base em perfis (o que inclusive é entendido como risco excessivo no Art. 13, I, c) [35], sendo mantido como alto risco apenas o uso de sistemas de IA para investigação e avaliação da credibilidade de provas. Em termos práticos, recomenda-se a seguinte alteração:

Art. 14. Considera-se de alto risco o sistema de IA empregado para as seguintes finalidades e contextos de usos, levando-se em conta a probabilidade e a gravidade dos impactos adversos sobre pessoas ou grupos afetados, nos termos de regulamentação: [...]

[31] BAHIA, Madalena Alexandre. *A criminalização de corpos negros no policiamento preditivo*: um estudo criminológico. Trabalho de Conclusão de Curso (Bacharelado em Direito)-Faculdade Nacional de Direito, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2024. Disponível em: https://pantheon.ufrj.br/bitstream/11422/26333/1/MABahia.pdf

[32] DRESCH, Leonardo Antonio. POLICIAMENTO PREDITIVO E A VIOLAÇÃO DE DIREITOS HUMANOS: ESTUDO DE CASO DO SISTEMA DA ORACLE. In: *Congresso Internacional de Direitos Humanos de Coimbra*. 2021. Disponível em: https://www.trabalhoscidhcoimbra.com/ojs/index.php/anaiscidhcoimbra/article/view/519

[33] LUCENA, Pedro Arthur Capelari de. *Policiamento preditivo, discriminação algorítmica e racismo*: potencialidades e reflexos no Brasil. VI Simpósio Internacional Lavits, 2019. Disponível em: https://lavits.org/wp-content/uploads/2019/12/Lucena-2019-LAVITSS.pdf

[34] MELO, Paulo Vctor. *A serviço do punitivismo, do policiamento preditivo e do racismo estrutural*. Le Monde Diplomatique Brasil (online). Publicado em 18/03/2021. Acesso em 14/01/2026. Disponível em: https://diplomatique.org.br/a-servico-do-punitivismo-do-policiamento-preditivo-e-do-racismo-estrutural/

[35] Art. 13. São vedados o desenvolvimento, a implementação e o uso de sistemas de IA:
I – com o propósito de:
[...] c) avaliar os traços de personalidade, as características ou o comportamento passado, criminal ou não, de pessoas singulares ou grupos, para avaliação de risco de cometimento de crimes, de infrações ou de reincidência;

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.cgi.br

X – investigação por autoridades administrativas para avaliar a credibilidade dos elementos de prova no decurso da investigação ou da 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~~;

2.1.5. Ranqueamentos para elegibilidade para políticas públicas: ajustes redacionais

No capítulo III, referente à categorização dos riscos, o PL acertadamente enquadra como risco excessivo — e portanto veda — o desenvolvimento, a implementação e o uso de sistemas de IA "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" (Artigo 13, II, grifo nosso).

Como ponto de aprimoramento, sugerimos a **remoção do trecho** "de forma ilegítima ou desproporcional", por considerar que sistemas de pontuação universal para acesso a bens e serviços e políticas públicas são intrinsecamente ilegítimos, não sendo possível serem proporcionais. Tal condicionalidade, portanto, é desnecessária e poderia se tornar uma brecha na formulação atual. Isso porque, na medida em que se condiciona o acesso a bens e serviços e políticas públicas a determinados comportamentos ou atributos, ou o incorporam a sistemas de pontuações, o que ocorre é que tais direitos deixam de ser inalienáveis, tal como previsto na Constituição, para se tornarem contingentes[36] — produzindo efeitos gravíssimos.

Em linha semelhante, passando para o Artigo 14, inciso IV, considera-se como **alto risco** o sistema de IA empregado para as seguintes finalidades e contextos de usos: "**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 à prestação de serviços públicos de assistência e de seguridade".

De fato, no que concerne a serviços públicos essenciais, concordamos que se deve considerar o emprego de sistemas de IA como de alto risco, considerando o papel fundamental que estes representam para a população. Como ponto de melhoria na redação, sugerimos apenas que, no trecho "avaliar a elegibilidade de pessoas naturais quanto **à prestação de** serviços (...)", o termo "prestação" seja substituído por "ao acesso a" serviços. Entendendo que a elegibilidade à qual o trecho se refere é para que as pessoas naturais acessem tais serviços, e não para que se tornem prestadoras, a alteração traria mais clareza para o texto.

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

[36] FREIRE, Nuno Nabais. *O Crédito Social*: uma ameaça ao Estado de Direito e às nossas liberdades. O Observador (online). Publicado em 30/09/2025. Acesso em 14/01/2026. Disponível em: https://observador.pt/opiniao/o-credito-social-uma-ameaca-ao-estado-de-direito-e-as-nossas-liberdades/

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.cgi.br

II – 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~~;

Art. 14. Considera-se de alto risco o sistema de IA empregado para as seguintes finalidades e contextos de usos, levando-se em conta a probabilidade e a gravidade dos impactos adversos sobre pessoas ou grupos afetados, nos termos de regulamentação: [...] 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~~ ao acesso a serviços públicos de assistência e de seguridade;

2.1.6. Análises automatizadas de crédito devem ser classificadas como de alto risco

Há um uso marcante de sistemas de Inteligência Artificial que não está elencado entre as situações de alto risco no PL 2.338/2023, embora possua alto impacto sobre as pessoas. Birôs de crédito, como o Serasa ou SPC Brasil, calculam uma **pontuação de crédito** de toda a população, para predizer a probabilidade de pagamento e o grau de confiabilidade dos consumidores, feita com base em complexos sistemas de aprendizado de máquina e enormes bases de dados.

Além de aplicações em situações diversas — para determinar compras à crédito, financiamento de imóvel, contratação de seguro, até mesmo em seleções de emprego —, o método automatizado para classificações pode imobilizar socialmente grupos mais vulneráveis, realizando classificações com alto potencial discriminatório[37]. Em relatório do modelo Mosaic, o Serasa chegou a informar que categorizava a população em grupos que vão de "Ricos, sofisticados e influentes", a "envelhecendo na periferia" e "aspirantes sociais" e subcategorias, como "Consumidores indisciplinados", "Excluídos do sistema" e "A pequena Alemanha no Brasil"[38] — todas classificações carregadas de significados políticos e sociais que podem imbuir uma série de discriminações ilícitas.

Essas previsões são feitas com base em generalizações que, embora facilitem a identificação de clientes com alto risco de inadimplemento, podem ocasionar discriminações. A impossibilidade de indivíduos pedirem explicações ou demonstrarem que as generalizações atribuídas a eles não se aplicam — todos deveres relacionados a sistemas de IA de alto risco — tornaria a situação ainda mais gravosa.

[37] Trabalhos como KREMER, B. Discriminações do sistema de pontuação de crédito: uma perspectiva de gênero e raça. In: OMS, J. *O consumidor na Era da Pontuação de Crédito*. Belo Horizonte, MG: Editora Letramento, 2022 e VILARINO, R. *Pontuações de crédito, aprendizagem de máquina e os riscos de alocar recursos predizendo o passado*. In: OMS, J. O consumidor na Era da Pontuação de Crédito. Belo Horizonte, MG: Editora Letramento, 2022, indicam a potencialidade de discriminação racial a partir do uso de dados como localização geográfica e CEP das pessoas em processos automatizados de pontuação de crédito.

[38] ZANATTA, R. A. (org.). *Por trás da pontuação de crédito*: conheça seus direitos. Instituto Brasileiro de Defesa do Consumidor. São Paulo: Idec, 2017.

Av. das Nações Unidas, 11.541
7º andar - Brooklin Novo
04578-000 - São Paulo - SP
tel: 55 11 **5509 3511**
fax: 55 11 **5509 3512**
www.cgi.br

Nesse sentido, **recomenda-se a inclusão de um inciso no Art. 14 do PL 2.338/2023, para prever que análises, pontuações ou ranqueamentos de crédito realizadas com o usos de sistemas de IA sejam classificadas como de alto risco**.

Art. 14. Considera-se de alto risco o sistema de IA empregado para as seguintes finalidades e contextos de usos, levando-se em conta a probabilidade e a gravidade dos impactos adversos sobre pessoas ou grupos afetados, nos termos de regulamentação: [...] XIII: análises, pontuações ou ranqueamentos para avaliação de crédito produzidas, com o envolvimento determinante, de sistemas de IA. Parágrafo único. Não se considera uso de alto risco aquele no qual o sistema de IA é utilizado como tecnologia intermediária que não influencie ou determine resultado ou decisão ou quando desempenha uma tarefa processual restrita.

* * *

CONCLUSÃO

O CGI.br reitera a disposição em colaborar com qualquer discussão sobre o tema, mantendo seu compromisso de atuar como espaço multissetorial e participativo para a governança da Internet no país, conforme estabelecido no Decreto nº 4.829/2003 e em linha com as provisões do Marco Civil da Internet no Brasil (Lei nº 12.965/2014, art. 24).