

Introdução

Este documento apresenta posicionamento da ANPD sobre o debate da regulação da inteligência artificial (IA) no Brasil. Com relação ao tema, desde a proposição do PL nº 21/2020, a discussão evoluiu bastante. Foi formada no Senado Federal uma Comissão de Juristas responsável por subsidiar elaboração de substitutivo sobre inteligência artificial (CJSUBIA) em 2022, o que representou importante avanço, pois a partir dela foram realizadas diversas audiências públicas, reunindo mais de 50 (cinquenta) especialistas, em formato multissetorial, contando com a participação de representantes do poder público, setor empresarial, sociedade civil e comunidade científico-acadêmica. A ANPD se orgulha de a Diretora Miriam Wimmer ter composto a Comissão. O relatório final da CJSUBIA, com mais de 900 páginas, incluiu um anteprojeto de lei que, em 03 de maio de 2023, foi convertido no PL nº 2338/2023, apresentado pelo Presidente do Senado Federal, o Senador Rodrigo Pacheco.

A ANPD avalia que o PL 2338/2023 possui diversos pontos de interação com a LGPD, notadamente no que diz respeito à tutela de direitos, à classificação de sistemas de IA de alto-risco e aos mecanismos de governança. Além disso, a Autoridade apoia o fomento à inovação, como a proposta de criação de ambientes de regulação experimental (*sandboxes* regulatórios)¹, desde que sejam desenhados com o propósito de promover a inovação responsável. Finalmente, a ANPD entende que, devido à sua função de guardião dos direitos à privacidade e à proteção de dados pessoais, é autoridade-chave na regulação de inteligência artificial. Nas seções a seguir, apresentam-se os argumentos que fundamentam esses posicionamentos.

¹ *Sandboxes* regulatórios são ambientes regulatórios experimentais, funcionando como colaborações que reúnem reguladores e organizações que desenvolvem novas tecnologias e processos para testar as inovações em relação à estrutura regulatória. DATASPHERE INITIATIVE. **Sandboxes for data: creating spaces for agile solutions across borders**. Disponível em: <https://www.thedatasphere.org/datasphere-publish/sandboxes-for-data/>.

O PL nº 2338/2023 possui diversos pontos de interação com a LGPD

Conforme consta na justificativa do PL nº 2338/2023, a proposta estabelece uma regulação baseada em riscos e uma modelagem regulatória baseada em direitos. Parte da premissa de que *“não há um trade-off entre a proteção de direitos e liberdades fundamentais, da valorização do trabalho e da dignidade da pessoa humana face à ordem econômica e à criação de novas cadeias de valor. Pelo contrário, seus fundamentos e a sua base principiológica buscam tal harmonização, nos termos da Constituição Federal”*. Essa opção de política regulatória é acertada e traça uma importante aproximação com a normativa brasileira de proteção de dados pessoais, que também compatibiliza a abordagem baseada em direitos (*rights-based approach*) com a abordagem baseada no risco (*risk-based approach*)², visto que ambas não são excludentes entre si.

Nesse sentido, o PL nº 2338/2023, a um só tempo, proíbe sistemas de IA de risco excessivo, delimita quais são os sistemas ditos de alto risco e suas obrigações e prevê direitos às pessoas naturais afetadas pelo funcionamento desses sistemas.

Por sua vez, a LGPD estabelece diferenças de regime jurídico ou de carga regulatória com base no nível de riscos gerado pela atividade de tratamento de dados executada pelo agente de tratamento, por exemplo, a obrigação de elaborar relatório de impacto à proteção de dados pessoais (RIPD) pelo controlador³. Além disso, a normativa garante um conjunto de direitos aos titulares⁴, ainda que a atividade de tratamento implique baixo risco a direitos, garantias e liberdades fundamentais da pessoa natural.

Outro ponto de interação que merece destaque entre a LGPD e o PL são os mecanismos de governança previstos, como o RIPD e a avaliação de impacto algorítmico (vide item 2.3), respectivamente, que auxiliam a promover estruturalmente nas organizações a conformidade ao regime de proteção de dados e às determinações da proposta de marco legal de IA.

² HUSTINX, Peter. EU Data Protection Law: The Review of Directive 95/46/EC and the General Data Protection Regulation. In: CREMONA, Marise (Coord.). **New Technologies and EU Law**. Oxford: Oxford University Press, 2017. p. 159-160; GELLERT, Raphaël. We Have Always Managed Risks in Data Protection Law. **European Data Protection Law Review**, v. 2, n. 4, p. 481-492, 2017.

³ Art. 5º, XVII, da LGPD. Vide, ainda, instruções sobre o RIPD disponibilizados pela ANPD em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd#p9

⁴ Art. 17 e seguintes da LGPD.

Sendo assim, três campos de correspondência entre o PL e a LGPD devem ser destacados, dada a possibilidade de eventuais convergências, sobreposições e conflitos com as atribuições legais da ANPD quando sistemas de IA realizarem tratamento de dados pessoais: (i) direitos da pessoa afetada por sistema de IA e os direitos dos titulares; (ii) a correlação entre sistemas de IA de alto risco e o tratamento de dados pessoais; e (iii) mecanismos de governança.

Tutela de direitos no PL nº 2338/2023 e os direitos dos titulares na LGPD

Dentre os direitos dispostos no PL, chamam atenção os **direitos à informação, à explicação, e à contestação e de solicitar revisão**. Trata-se de direitos que se destinam à tutela das pessoas naturais afetadas por sistemas de IA e que possuem similaridades com alguns dispositivos da LGPD relativos aos direitos dos titulares (vide Anexo 1, Tabela 1). As semelhanças, na verdade, abrem espaço a convergências bem como a possíveis conflitos.

A proposta legislativa estabelece que **à pessoa afetada devem ser asseguradas informações claras e adequadas**, previamente à contratação ou utilização do sistema de IA, sobre uma série de aspectos, tais como: (i) o caráter automatizado da interação com o sistema, (ii) sua descrição geral, e (iii) os tipos de decisões, recomendações ou previsões que se destina a fazer e consequências de sua utilização para a pessoa natural. Ainda, deve haver a identificação dos operadores do sistema de IA e informação sobre medidas de governança adotadas no desenvolvimento e emprego do sistema.

A tutela desse direito previsto no PL tem relação com o **direito de acesso**, consagrado no art. 9º da LGPD, que também garante ao titular de dados o recebimento de informações relevantes sobre as operações de tratamento de seus dados pessoais. Tais informações devem ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outros aspectos, a finalidade específica do tratamento, a forma e duração do tratamento. Ademais, nos dois casos remete-se à posterior regulamentação a respeito de informações adicionais, a ser criada pela autoridade competente.

Os recentes casos de investigação de aplicações baseadas em IA generativa (por exemplo, os grandes modelos de linguagem – *large language models*, como o ChatGPT) por autoridades de proteção de dados como a italiana⁵, a espanhola⁶ e a canadense⁷, já evidenciam a importância de se assegurar acesso a

⁵ <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9881490?s=08#english>

⁶ <https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/aepd-inicia-de-oficio-actuaciones-de-investigacion-a-openai>

⁷ https://priv.gc.ca/en/opc-news/news-and-announcements/2023/an_230404/

informações adequadas para o exercício de direitos do titular cujos dados pessoais são objeto de tratamento por tais sistemas de IA. A Rede Iberoamericana de Proteção de Dados também iniciou, em maio deste ano, uma ação coordenada para garantir a proteção de direitos e liberdades de indivíduos afetados pelo ChatGPT⁸.

Com relação ao **direito de contestação e de solicitar revisão**, o texto do PL possui direta correspondência com o **direito de solicitar a revisão** de decisões automatizadas previsto no artigo 20 da LGPD. O confronto de ambos, contudo, aponta para uma possível tensão. No primeiro, o direito de contestar e de solicitar a revisão de decisões, recomendações ou previsões geradas por sistema de IA é garantido desde que produzam “**efeitos jurídicos relevantes**” ou que “**impactem de maneira significativa os interesses da pessoa**” (art. 9º). Já a previsão normativa da LGPD estabelece que o direito de revisão se aplica em hipóteses de “decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que **afetem seus interesses**”, a exemplo do que ocorre nos casos de perfilamento.

Tendo em vista que o PL estipula requisitos mais estritos e não menciona o artigo 20 da LGPD, eventual aprovação da proposta causaria incerteza jurídica nas situações em que sistemas de IA tratam dados pessoais. É necessário, portanto, que a compatibilidade jurídica seja estabelecida pelo PL, assegurando-se o respeito às competências da ANPD em regular o tema que já lhe é afeto.

Percebe-se, ainda, notória convergência entre o dever imposto no artigo 20, § 1º, da LGPD, aos controladores no contexto de tomada de decisão automatizada, e o **direito à explicação** sobre a decisão, previsão ou recomendação, com informações a respeito dos critérios e dos procedimentos utilizados, assim como sobre os principais fatores que afetam tal previsão ou decisão específica. Desse modo, a ANPD possui papel relevante na regulação do direito à explicação.

Por fim, cabe mencionar que tanto o PL nº 2338/2023 (art. 3º, IV) quanto a LGPD (art. 6º, IX) mencionam o princípio da **não discriminação**. No caso do PL, esse princípio é ainda mencionado como fundamento (art. 2º, V) e direito (art. 5º, V). No contexto da revisão de decisões automatizadas, conforme o art. 20, §2º, da LGPD, a ANPD possui competência para realizar auditorias com o objetivo de verificar se existem aspectos discriminatórios no tratamento automatizado. Além disso, o PL nº 2338/2023 define discriminação como

⁸ <https://www.redipd.org/es/noticias/autoridades-red-iberoamericana-de-proteccion-de-datos-personales-inician-accion-chatgpt>

[...] 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** (grifou-se).

Ao assim fazê-lo, o PL associa os efeitos discriminatórios aos usos ilegítimos e abusivos de dados pessoais sensíveis, definidos no art. 5º, II, da LGPD. Assim, fica claro que a identificação de efeitos discriminatórios de sistemas de inteligência artificial envolve, necessariamente, uma avaliação dos riscos associados ao tratamento de dados pessoais sensíveis, tema cuja competência regulatória é afeta à ANPD.

IAs de alto risco e tratamento de dados pessoais

O PL em discussão, em modelo semelhante ao *AI Act* europeu, aborda classificações de risco excessivo e risco alto, delimita a regulação consoante os desdobramentos de risco da tecnologia e considera que diferentes níveis de risco justificam diferentes níveis de restrições, garantias e salvaguardas proporcionais. Em algumas circunstâncias, o risco pode ser tão alto que, por precaução, pode ser necessário proibir o desenvolvimento ou uso de aplicativos dessas tecnologias, trazendo, inclusive, o conceito de riscos inaceitáveis.

O PL apresenta um rol de finalidades de uso categorizadas como de alto risco, delegando o processo contínuo de atualização desse rol por meio de critérios específicos direcionados à autoridade competente.

Uma característica frequente nos sistemas considerados de alto risco é **o tratamento de dados pessoais e de dados sensíveis**. Vários dos sistemas de inteligência artificial considerados de alto risco envolvem o tratamento de dados pessoais porque eles são projetados para tomar decisões automatizadas que podem ter um impacto significativo em direitos e interesses de indivíduos, como por exemplo, decisões relacionadas a crédito, emprego, segurança pública e saúde. Esses sistemas geralmente são treinados por meio de bases de dados com grandes quantidades de dados pessoais, como informações de identificação pessoal, histórico de compras, atividades realizadas *online* e até mesmo dados biométricos. Esses dados são usados para treinar algoritmos e ajudá-los a identificar padrões e tomar decisões mais precisas.

Salienta-se que dois dos critérios estabelecidos pelo PL para que a autoridade competente atualize as listas dos sistemas de IA de risco excessivo ou de alto risco envolvem expressamente a utilização de dados pessoais: (i) alto nível de identificabilidade dos titulares dos dados; e (ii) quando existirem expectativas razoáveis do afetado quanto ao uso de seus dados pessoais.

A IA é uma tecnologia estratégica, que oferece muitos benefícios para a sociedade. Claramente, existem ganhos de eficiência e produtividade que podem fortalecer a competitividade dos negócios e melhorar o bem-estar das pessoas. Portanto, as questões de proteção de dados devem ser consideradas desde o início e monitoradas ao longo dos ciclos de vida dos sistemas de IA para garantir a conformidade com os direitos humanos e direitos fundamentais⁹.

Por essa razão, existe uma preocupação regulatória especial com os efeitos desses sistemas de IA para os direitos fundamentais não apenas de seus usuários imediatos, mas de indivíduos e grupos que eventualmente estejam sujeitos às decisões desses sistemas. Direitos como a não discriminação, a privacidade, a proteção de dados pessoais e até mesmo o acesso a determinados benefícios sociais podem ser afetados por essas decisões automatizadas.

Para ilustrar o potencial negativo do mal uso de IA no âmbito de dados pessoais, em 2018, a Amazon lançou um sistema de reconhecimento facial chamado Rekognition, que foi usado por algumas autoridades policiais nos Estados Unidos. Estudos mostraram que o sistema apresentava uma taxa de erro maior para identificar rostos de pessoas negras, especialmente mulheres. Isso pode ter resultado em pelo menos 28 falsas acusações e prisões injustas¹⁰.

No mesmo ano de 2018, a Amazon abandonou uma ferramenta de recrutamento de pessoas baseada em um sistema de IA, que favorecia homens para trabalhos técnicos¹¹. Especialistas vinham desenvolvendo o sistema desde 2014 para revisar currículos em um esforço para automatizar esse processo de busca, mas a ferramenta de contratação automatizada da Amazon foi considerada inadequada após penalizar os currículos de candidatas (especialmente mulheres negras) e favorecer candidatos homens.

Mecanismos de Governança

Com relação aos mecanismos de governança dos sistemas de IA propostos no PL nº 2338/2023, vários deles apresentam sinergia com obrigações previstas na LGPD. No Anexo 1, Tabela 2, apresenta-se um comparativo das medidas previstas no PL com dispositivos da LGPD.

⁹ KUNER, Christopher; CATE, Fred H.; LYNSEY, Orla; MILLARD, Christopher; LOIDEAIN, Nora Ni; SVANTESSON, Dan Jerker B. Expanding the artificial intelligence-data protection debate. **International Data Privacy Law**, v. 8, n. 4, p. 289–292, nov. 2018. Disponível em: <https://doi.org/10.1093/idpl/ipy024>.

¹⁰ Ver tabela comparativa 2 do Anexo a esta Nota Técnica.

<https://www.theguardian.com/technology/2018/jul/26/amazon-facial-rekognition-congress-mugshots-aclu>.

¹¹ <https://www.theguardian.com/technology/2018/oct/10/amazon-hiring-ai-gender-bias-recruiting-engine>.

A análise comparada permite observar que **as medidas de governança propostas pelo PL dialogam diretamente com diversos dispositivos da LGPD**: (i) os princípios previstos no art. 6º, tais como transparência, segurança e não discriminação; (ii) os direitos dos titulares, em particular os relativos a decisões baseadas em tratamento automatizado de dados pessoais (art. 20); e (iii) o princípio da privacidade desde a concepção (*privacy by design*), implícito no art. 46, §2º. Ainda, é evidente certo paralelismo entre as disposições sobre a instituição de **programas de governança mediante códigos de conduta de agentes de IA** (art. 30 do PL) com a disciplina da LGPD sobre regras de boas práticas e governança em proteção de dados, que estabelece, em seu art. 50, §2º, inciso I, o **programa de governança em privacidade**. Em ambos os casos se denota a escolha de política legislativa em favor da **autorregulação regulada**, a fim de promover nos agentes regulados atitude preventiva e de antecipação de riscos a direitos e liberdades fundamentais.

Outro instrumento de governança que exige reflexão é a **avaliação de impacto algorítmico (AIA)**, discriminada em seção específica do PL. Conquanto o texto não apresente uma definição do termo, a metodologia para sua elaboração é apresentada, sendo composta pelas seguintes etapas: (i) preparação; (ii) cognição do risco; (iii) mitigação dos riscos encontrados; e (iv) monitoramento. Como toda avaliação de impacto, trata-se de uma ferramenta que permite ao agente descrever características do sistema analisado, bem como identificar riscos e mecanismos para sua mitigação.

A LGPD também apresenta um instrumento análogo, qual seja, o **relatório de impacto à proteção de dados pessoais (RIPD)**, definido no art. 5º, XVII, como a *“documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco”*. Por sua vez, o art. 38, parágrafo único, da LGPD, apresenta qual deve ser seu conteúdo mínimo: (i) a descrição dos tipos de dados coletados; (ii) a metodologia utilizada para a coleta e para a garantia da segurança das informações; e (iii) a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

Embora o escopo de tratamento de um RIPD seja restrito a contextos que envolvam tratamento de dados pessoais e sua análise limitada à gestão de riscos a liberdades e direitos fundamentais afetados em virtude deste tratamento, é indubitável a correlação entre as duas ferramentas, tanto no aspecto metodológico de sua elaboração, quanto no conteúdo (para os casos em que sistemas de IA tratem dados pessoais). Por exemplo, é possível citar tecnologias de reconhecimento facial e aplicações de IA na área da saúde, que certamente exigirão a elaboração de AIA e RIPD.

Em relatório recente sobre esse instrumento¹², o Laboratório de Políticas Públicas e Internet – LAPIN, comenta que, como a AIA é usada para gerir riscos de sistemas de IA a direitos fundamentais, inevitavelmente, os direitos à privacidade e à proteção de dados pessoais devem ser considerados na análise.

Deste modo, é pertinente observar que, seja qual for a autoridade supervisora de IA, ela deverá estar alinhada às atividades regulatórias da ANPD, para garantir que os instrumentos de governança para regulação da IA sejam compatíveis com os princípios, obrigações e mecanismos de governança da LGPD, tais como a elaboração de RIPD em casos de tratamento de dados pessoais de alto risco.

O fomento à inovação em IA é importante, desde que promova o desenvolvimento de inovações responsáveis

Sabe-se que a arquitetura regulatória costuma ser criticada por trazer barreiras para a inovação. Por isso, uma preocupação dos reguladores contemporâneos é **estabelecer estruturas que compatibilizem o fomento à inovação com a proteção de direitos fundamentais**.

No cenário internacional, importante exemplo pode ser trazido da União Europeia (UE), que, em 2015, lançou a estratégia do Mercado Único Digital, um esforço de integração de seus Estados membros no que diz respeito a políticas de **incentivo à inovação** e à regulação de ferramentas e serviços digitais. Fundada em pilares como acesso, segurança, proteção de dados, crescimento da economia digital e transparência das plataformas, a estratégia passou a abarcar iniciativas legislativas paradigmáticas, como, por exemplo, o Regulamento Geral de Proteção de Dados (2016)¹³, a Diretiva sobre Direitos Autorais e Direitos Conexos

¹² LAPIN. **Relatório sobre avaliação de impacto algorítmico para proteção dos direitos fundamentais** (2023). Disponível em: <https://lapin.org.br/2023/04/13/avaliacao-de-impacto-algoritmico-para-protecao-dos-direitos-fundamentais/>. Acesso em: 19 abr. 2023.

¹³ <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679>

(2019)¹⁴, a Lei dos Serviços Digitais (2022)¹⁵, a Lei dos Mercados Digitais (2022)¹⁶, e, mais recentemente, a proposta de Regulamento Geral da Inteligência Artificial (AI Act)¹⁷, que ainda está em discussão no Parlamento europeu.

A ideia de uma estratégia para o Mercado Único Digital é facilitar o fluxo de informações e acesso a serviços digitais intrabloco, maximizar o potencial de crescimento da economia digital da UE, reposicionar o continente no cenário econômico digital global, bem como influenciar a criação de padrões internacionais de regulação conforme seus próprios interesses. Ou seja, há um esforço de coordenação entre as diferentes etapas de regulamentação digital no bloco, de forma a pensar essa estratégia **sob seus mais variados aspectos**: consumerista, concorrencial, político, de propriedade intelectual, de proteção de direitos fundamentais, entre outros.

É essencial que a mesma preocupação sistêmica esteja presente nos esforços legislativos e regulatórios na jurisdição brasileira. Além da necessidade de compatibilização das sobreposições das regras propostas pelo PL nº 2338/2023 com a LGPD, **o fomento à inovação também se torna peça-chave do debate regulatório de novas tecnologias, desde que esse fomento promova o desenvolvimento de inovações responsáveis**. Por exemplo, em relatório publicado em março de 2023, o governo do Reino Unido anunciou que irá fomentar *sandboxes* de IA que promovam a inovação responsável e que permitam interoperabilidade entre as iniciativas dos agentes reguladores.

Nesse sentido, a decisão do PL de trazer seção específica sobre o tema é acertada. Com o objetivo de criar um ambiente regulatório que seja propício à inovação, a proposta apresenta medidas para fomentá-la, destacando a possibilidade de implementação de *sandboxes* regulatórios.

De forma cautelosa, o PL não antecipa muitas regras sobre esse tema, estabelecendo que a autoridade supervisora competente irá autorizar o funcionamento de *sandboxes* que preencham os requisitos especificados pela lei e por regulamentação futura. Isso permite que diversos reguladores proponham seus projetos de *sandbox*, de forma que iniciativas distintas possam ser fomentadas de acordo com o setor regulado (por exemplo, na saúde ou nas telecomunicações).

Além disso, o PL apresenta características mínimas que os projetos de *sandbox* devem conter, quais sejam:

- (i) inovação no emprego da tecnologia ou no uso alternativo de tecnologias existentes; (ii)

¹⁴ <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32019L0790>

¹⁵ <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32022R2065>

¹⁶ <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32022R1925>

¹⁷ <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52021PC0206>

aprimoramentos no sentido de ganhos de eficiência, redução de custos, aumento de segurança, diminuição de riscos, benefícios à sociedade e a consumidores, entre outros; e (iii) plano de descontinuidade, com previsão de medidas a serem tomadas para assegurar a viabilidade operacional do projeto uma vez encerrado o período da autorização do *sandbox* regulatório.

Define ainda que a edição de regulamentação e recomendações sobre *sandboxes* de IA é atribuição da autoridade competente, e que os participantes do *sandbox* continuam sendo responsáveis por quaisquer danos infligidos a terceiros em resultado da experimentação que ocorra no ambiente de testagem. Assim, os regimes de responsabilidade continuam vigentes.

Seria importante que o PL desse maior destaque às questões relativas à proteção de dados nos *sandboxes* de IA que tratem dados pessoais, visto que este é o caso de diversos sistemas de IA de alto risco. Nesse sentido, em maio deste ano, a ANPD começou a desenvolver estudos de projeto-piloto de ambiente regulatório experimental com esse exato recorte¹⁸.

No contexto europeu, a fim de garantir o cumprimento das legislações de proteção de dados, o *AI Act* apresenta, no artigo 54, requisitos para posterior tratamento de dados pessoais com finalidade diversa da original em *sandboxes* de IA. Além de limitar o escopo do tratamento posterior a circunstâncias específicas de interesse público (prevenção do crime, segurança pública, saúde pública e proteção do meio ambiente), a norma exige a implementação de várias salvaguardas, como a existência de mecanismos de monitoramento eficazes para identificar se riscos elevados para os direitos fundamentais dos titulares dos dados podem surgir durante a testagem, além do isolamento dos ambientes de tratamento de dados pessoais durante a experimentação.

Ademais, a proposta europeia prevê no artigo 53(2) que as Autoridades de Proteção de Dados (APDs) devem estar envolvidas nos *sandboxes*, independentemente de serem designadas como autoridade competente da IA, quando a inovação em teste envolver o tratamento de dados pessoais. Essa proposta torna as APDs guardiãs dos *sandboxes* regulatórios de IA na UE e é compatível com iniciativas que já vêm sendo realizadas no contexto europeu, mencionadas em seção anterior.

No contexto brasileiro, **é fundamental que alguma previsão similar à proposta europeia inclua papel de destaque da ANPD em *sandboxes* de IA que envolvam inovações que tratem dados pessoais.**

¹⁸ <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-formaliza-cooperacao-tecnica-com-o-banco-de-desenvolvimento-da-america-latina-2013-caf>

A ANPD é autoridade-chave na regulação de inteligência artificial e proteção de dados pessoais

O PL estabelece que caberá ao Poder Executivo designar autoridade competente para zelar pela implementação e fiscalização da lei proposta (art. 32). Ela contará com atribuições específicas dispostas no texto, como, por exemplo: (i) zelar pela **proteção a direitos fundamentais** e a demais direitos afetados pela utilização de sistemas de IA; (ii) promover a elaboração, atualização e implementação da Estratégia Brasileira de Inteligência Artificial **junto aos órgãos de competência correlata**; (iii) promover ações de cooperação com **autoridades de proteção** e de fomento ao desenvolvimento e à utilização dos sistemas de IA de outros países, de natureza internacional ou transnacional; (iv) expedir normas para a regulamentação da lei, inclusive sobre procedimentos associados ao **exercício dos direitos** nela previstos, e **forma e requisitos das informações a serem publicizadas** sobre a utilização de sistemas de IA; e (v) solicitar, a qualquer momento, às entidades do poder público que desenvolvam ou utilizem sistemas de IA, **informações a respeito da natureza dos dados e dos demais detalhes do tratamento realizado**.

Quanto à competência fiscalizatória prevista no artigo 32, VII, do PL, cumpre destacar dois temas convergentes entre a proposta legislativa e a LGPD: (i) comunicação de incidentes de segurança e (ii) sanções administrativas.

À semelhança do dever de o controlador comunicar à ANPD a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, estabelecido no artigo 48, da LGPD, o PL propõe a imposição da obrigação de se comunicar à autoridade competente *“a ocorrência de graves incidentes de segurança, incluindo quando houver risco à vida e integridade física de pessoas, a interrupção de funcionamento de operações críticas de infraestrutura, graves danos à propriedade ou ao meio ambiente, bem como graves violações aos direitos fundamentais”* (art. 31). Além disso, muito aproximados, senão equivalentes, são os regimes de direito administrativo sancionador aplicáveis aos agentes infratores da normativa de proteção de dados e dos preceitos do PL.

Como é possível observar no texto acima, as atribuições definidas para a autoridade competente em IA guardam estreitas semelhanças com as atribuições legais da ANPD, especialmente quando se referem à natureza dos dados tratados e à proteção a direitos fundamentais, temas centrais a esta Autoridade, o

que suscita potenciais conflitos com as competências legais da ANPD previstas na LGPD. Essa semelhança está detalhada no Anexo 1, Tabela 3.

Assim, a eventual criação de um novo órgão regulador ou a atribuição de competências a outra entidade pública teria por efeito gerar uma fragmentação regulatória e uma sobreposição de competências com a ANPD.

Por exemplo, um mesmo tema, como os direitos à informação, à explicação e à contestação e de solicitar revisão, poderia ser objeto de regulamentação simultânea pela ANPD e pela autoridade competente de IA. Situação semelhante poderia ocorrer em relação aos mecanismos de governança.

Ou, ainda, um mesmo agente poderia ser sancionado por ambas as entidades reguladoras diante de uma mesma conduta, o que pode suscitar questionamentos judiciais, comprometendo-se a efetividade da regulação estatal e do objetivo de proteger direitos dos afetados pelos sistemas de IA.

Cabe destacar que, nos termos da LGPD, **a aplicação das sanções referente à proteção de dados pessoais compete exclusivamente à ANPD, e suas competências prevalecerão, no que se refere à proteção de dados pessoais, sobre as competências correlatas de outras entidades ou órgãos da administração pública.**

Diante dos pontos apresentados, a ANPD ressalta a alta relevância da convergência regulatória do regramento da LGPD e do futuro marco legal de IA, especialmente no que diz respeito à autoridade competente.

Partindo do ponto de vista da experiência da ANPD, centralizar a garantia da proteção de dados e da privacidade com a governança em matéria de IA demonstra ser o caminho mais adequado para a sustentação da segurança jurídica, promovendo coerente e sistemática interpretação dos marcos normativos que permitam assegurar um nível de maior uniformidade regulatória entre temas fortemente interligados, evitando, assim, riscos de fragmentação regulatória. É preciso, ainda, acrescentar que essa é uma demanda econômica relevante, tendo em vista que, quanto mais consistente a uniformização, maior o potencial de reduzir o custo em adequação exigida pelo regramento, com possível efeito no aumento da confiança dos agentes regulados e população geral no uso de sistemas de IA.

Esse ponto repercute na atuação institucional diante de atores interessados em eventos, acordos de cooperação e ações diversas. Partindo do princípio de que tanto a proteção de dados pessoais quanto a regulação de IA operam de forma participativa e multisetorial, nacional e internacionalmente, e de que são temas convergentes, o diálogo e a negociação da estratégia regulatória brasileira com atores

domésticos e estrangeiros precisam ser realizados de forma harmônica, o que se beneficiaria em ter uma única autoridade responsável.

Internacionalmente existe manifestação nesse sentido emanada em nota conjunta pela Autoridade Europeia de Proteção de Dados (*European Data Protection Supervisor – EDPS*, no original) e pelo Comitê Europeu de Proteção de Dados (*European Data Protection Board – EDPB*, no original)¹⁹. Elas esclarecem que **designar a autoridade de proteção de dados como autoridade supervisora de IA é uma estratégia que assegura não só harmonia na regulamentação, como também uma interpretação coerente das disposições perante os sujeitos regulados**. Dessa forma, se posicionam no sentido de que é a melhor escolha a se fazer.

Ainda que não se caminhe nesse sentido, ou seja, que não se atribua à ANPD o papel de autoridade competente para fins de IA, é inegável que a ANPD, dadas as suas competências, é figura-chave na regulação de IA no Brasil. Nesse sentido, é possível notar na experiência internacional esforços das Autoridades de Proteção de Dados em utilizar das atribuições institucionais que já lhes competem para regulamentar questões afetas à regulação de sistemas de IA. Para além dos casos já citados de fiscalização de IA generativa pelas autoridades da Itália e Espanha, cabe citar a atuação da autoridade da Holanda,²⁰ que criou, em janeiro de 2023, unidade dedicada para poder lidar com questões de transparência e discriminação algorítmica, bem como articular a regulação do tema frente a outros setores regulados como o da saúde e das telecomunicações.

Além disso, as autoridades também têm se dedicado ao fomento da inovação responsável, incluindo sistemas de IA, como se pode destacar nas experiências dos *sandboxes* desenvolvidos pelas autoridades da Colômbia,²¹ França,²² Noruega,²³ Reino Unido²⁴ e Singapura.²⁵

Considerando a relevância que o uso de dados pessoais representa para o funcionamento de diversos sistemas de IA (vários deles de alto risco), é justo afirmar que existe uma sobreposição de competências a ser alinhada. Importa destacar que a ANPD já tem atuado em sistemas que possuem IA que tratam dados pessoais de forma a garantir proteção de direitos fundamentais. Isso evidencia que a Autoridade tem

¹⁹ https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf

²⁰ <https://iapp.org/news/a/dutch-dpa-begins-algorithm-enforcement-work/>

²¹ <https://www.sic.gov.co/sandbox-microsite>

²² <https://www.cnil.fr/fr/accompagnement-renforce-la-cnil-lance-un-nouveau-dispositif-innovant-daccompagnement>

²³ <https://www.datatilsynet.no/en/regulations-and-tools/sandbox-for-artificial-intelligence/>

²⁴ <https://ico.org.uk/sandbox>

²⁵ <https://iapp.org/news/a/singapore-imda-and-pdpc-announce-launching-of-pet-sandbox-for-businesses/>

mantido esforços no sentido de considerar em sua Agenda Regulatória questões associadas à IA (item 19 da Agenda Regulatória 2023/2024) e à avaliação de riscos a direitos fundamentais (itens 2, 5 e 8), demonstrando, portanto, perfil institucional para regular o tema em sua área de competência. Desse modo, **tanto a experiência comparada quanto a nacional apontam para a relevância da ANPD como autoridade-chave na regulação da IA para fins de garantir a proteção dos dados pessoais.**

Conclusão

Assim como no debate sobre a regulação de plataformas, a ANPD entende que sua competência na proteção dos direitos de titulares de dados deve ser respeitada no âmbito da regulação da IA. Além disso, tendo em vista a forte sinergia da proposta apresentada no PL 2338/2023 com os temas tratados na LGPD, esta Autoridade entende que possui papel-chave na governança da IA e proteção de dados pessoais.

Para isso, a LGPD e a futura regulação de IA devem estar em consonância, e a autoridade competente que irá regular essa tecnologia deverá respeitar o que já está disposto na LGPD.

A consolidação da ANPD como a autoridade-chave em matéria de IA e proteção de dados pessoais permitirá garantir essa consistência e a harmonia regulatória necessária para o fomento à inovação responsável e, principalmente, para a proteção dos dados pessoais e de outros direitos e liberdades fundamentais do titular.

Em síntese, por fim, são as conclusões e recomendações desta Autoridade:

- i. É imprescindível a compatibilização das sobreposições e conflitos existentes entre o PL e a LGPD, em especial no que concerne às atribuições legais da ANPD, inclusive as de caráter fiscalizatório. Entre os aspectos de maior atenção, destacam-se situações em que sistemas de IA realizam tratamento de dados pessoais, notadamente em matérias como os direitos da pessoa afetada por sistema de IA e os direitos dos titulares; a correlação entre sistemas de IA de alto risco e o tratamento de dados pessoais; e os mecanismos de governança de IA e de proteção de dados pessoais;
- ii. A fim de incentivar a inovação responsável é necessário que o PL disponha de forma mais específica sobre a proteção de dados pessoais nos *sandboxes* de IA que envolvam o tratamento desses dados, em especial quanto a sistemas de IA de alto risco, e as funções e atribuições a serem desempenhadas pela ANPD nos *sandboxes* regulatórios de IA que envolvam o tratamento de dados pessoais;

- iii. A fim de garantir segurança jurídica e convergência regulatória, é fundamental garantir o papel da ANPD como autoridade-chave no que se refere à regulação e à governança da IA no Brasil.

Como sempre, a ANPD se mantém disponível para o debate público e conta com a colaboração dos esforços multissetoriais para garantir a sua relevância na proteção da privacidade e da proteção de dados pessoais, inclusive nos contextos de tratamento por sistemas de IA.

ANEXO 1

Tabelas comparativas entre o PL nº 2338/2023 e a LGPD

A seguir são apresentadas três tabelas comparativas que facilitam a percepção das diversas similaridades entre o PL nº 2338/2023 e a LGPD. São elas:

- **Tabela 1:** Comparação entre os direitos da pessoa afetada pelo sistema de IA no PL nº 2338/2023 e os direitos dos titulares na LGPD
- **Tabela 2:** Comparação das medidas de governança do art. 19 do PL nº 2338/2023 com a LGPD
- **Tabela 3:** Comparação das competências da autoridade chave do PL nº 2338/2023 com às atribuídas à ANPD pela LGPD

Tabela 1: Comparação entre os direitos da pessoa afetada pelo sistema de IA no PL nº 2338/2023 e os direitos dos titulares na LGPD

PL nº 2338/2023	LGPD
<p>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:</p> <p>I – caráter automatizado da interação e da decisão em processos ou produtos que afetem a pessoa;</p> <p>II – descrição geral do sistema, tipos de decisões, recomendações ou previsões que se destina a fazer e consequências de sua utilização para a pessoa;</p> <p>III – identificação dos operadores do sistema de inteligência artificial e medidas de governança adotadas no desenvolvimento e emprego do sistema pela organização;</p> <p>IV – papel do sistema de inteligência artificial e dos humanos envolvidos no processo de</p>	<p>Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:</p> <p>I – finalidade específica do tratamento;</p> <p>II – forma e duração do tratamento, observados os segredos comercial e industrial;</p> <p>III – identificação do controlador;</p> <p>IV – informações de contato do controlador;</p> <p>V – informações acerca do uso compartilhado de dados pelo controlador e a finalidade;</p> <p>VI – responsabilidades dos agentes que realizarão o tratamento; e</p> <p>VII – direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.</p>

tomada de decisão, previsão ou recomendação;

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

VII – outras informações definidas em regulamento.

§ 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**.

Art. 19. A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular:

I – em **formato simplificado**, imediatamente; ou

II – por meio de **declaração clara e completa**, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular.

(...)

§ 2º As informações e os dados poderão ser fornecidos, a critério do titular:

I – por meio eletrônico, seguro e idôneo para esse fim; ou

II – sob forma impressa.

§ 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.

Sem correspondência direta.

§ 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.**

Art. 14. (...)

§ 6º As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, **consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.**

Art. 8º A pessoa afetada por sistema de inteligência artificial **poderá solicitar explicação sobre a decisão, previsão ou recomendação, com informações a respeito dos critérios e dos procedimentos utilizados**, assim como sobre os principais fatores que afetam tal previsão ou decisão específica, incluindo informações sobre:

I – a racionalidade e a lógica do sistema, bem como o significado e as consequências previstas de tal decisão para a pessoa afetada;

II – o grau e o nível de contribuição do sistema de inteligência artificial para a tomada de decisões;

III – os dados processados e a sua fonte, bem como os critérios para a tomada de decisão e, quando apropriado, a sua ponderação, aplicados à situação da pessoa afetada;

IV – os mecanismos por meio dos quais a pessoa pode contestar a decisão; e

V – a possibilidade de solicitar intervenção humana, nos termos desta lei.

Parágrafo único. As informações mencionadas no caput serão fornecidas por procedimento gratuito e facilitado, **em linguagem que permita que a pessoa compreenda o resultado da decisão ou previsão em questão**, no prazo de até quinze dias a contar da solicitação, permitida a prorrogação, uma vez, por igual período, a depender da complexidade do caso.

Art. 20. (...)

1º O controlador **deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada**, observados os segredos comercial e industrial.

Art. 9º A pessoa afetada por sistema de inteligência artificial terá o **direito de contestar e de solicitar a revisão de decisões**, recomendações ou previsões geradas por tal sistema que produzam **efeitos jurídicos relevantes** ou que impactem de **maneira significativa** seus interesses.

Art. 20. O titular dos dados tem **direito a solicitar a revisão de decisões** tomadas unicamente com base em tratamento automatizado de **dados pessoais** que afetem seus **interesses**, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

§ 1º Fica assegurado o **direito de correção de dados incompletos, inexatos ou desatualizados** utilizados por sistemas de inteligência artificial, assim como o **direito de solicitar a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a legislação**, nos termos do art. 18 da Lei no 13.709, de 14 de agosto de 2018 e da legislação pertinente.

Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: (...)

III - **correção de dados incompletos, inexatos ou desatualizados;**

IV - **anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei; (...)**

§ 2º O **direito à contestação** previsto no caput deste artigo **abrange também decisões, recomendações ou previsões amparadas em inferências discriminatórias, irrazoáveis ou que atentem contra a boa-fé objetiva**, assim compreendidas as inferências que:

I – sejam fundadas em dados inadequados ou abusivos para as finalidades do tratamento;

II – sejam baseadas em métodos imprecisos ou estatisticamente não confiáveis; ou

III – não considerem de forma adequada a individualidade e as características pessoais dos indivíduos.

Artigo 20, *caput* (vide acima)

Art. 10. Quando a decisão, previsão ou recomendação de sistema de inteligência artificial produzir efeitos jurídicos relevantes ou que impactem de maneira significativa os interesses da pessoa, inclusive por meio da

Sem correspondência direta.

geração de perfis e da realização de inferências, esta poderá **solicitar a intervenção ou revisão humana**.

Parágrafo único. **A intervenção ou revisão humana** não será exigida caso a sua implementação seja comprovadamente impossível, hipótese na qual o responsável pela operação do sistema de inteligência artificial implementará medidas alternativas eficazes, a fim de assegurar a reanálise da decisão contestada, levando em consideração os argumentos suscitados pela pessoa afetada, assim como a reparação de eventuais danos gerados.

Art. 11. Em cenários nos quais as decisões, previsões ou recomendações geradas por sistemas de inteligência artificial tenham um impacto irreversível ou de difícil reversão ou envolvam decisões que podem gerar riscos à vida ou à integridade física de indivíduos, haverá envolvimento **humano significativo no processo decisório e determinação humana final**.

Art. 12. As pessoas afetadas por decisões, previsões ou recomendações de sistemas de inteligência artificial têm **direito a tratamento justo e isonômico**, sendo vedadas a implementação e o uso de sistemas de inteligência artificial que possam acarretar discriminação direta, indireta, ilegal ou abusiva, inclusive:

I – em decorrência do uso de dados pessoais sensíveis ou de impactos desproporcionais em razão de características pessoais como origem geográfica, raça, cor ou etnia, gênero, orientação sexual, classe socioeconômica, idade, deficiência, religião ou opiniões políticas; ou

Sem correspondência direta.

Sem correspondência direta.

Sem correspondência direta.

II – em função do estabelecimento de desvantagens ou agravamento da situação de vulnerabilidade de pessoas pertencentes a um grupo específico, ainda que se utilizem critérios aparentemente neutros.

Parágrafo único. A vedação prevista no caput não impede a adoção de critérios de diferenciação entre indivíduos ou grupos quando tal diferenciação se dê em função de objetivos ou justificativas demonstradas, razoáveis e legítimas à luz do direito à igualdade e dos demais direitos fundamentais.

Tabela 2: Comparação das medidas de governança do art. 19 do PL nº 2338/2023 com a LGPD

PL nº 2338/2023	LGPD
Art. 19, I - medidas de transparência quanto ao emprego de sistemas de inteligência artificial na interação com pessoas naturais, o que inclui o uso de interfaces ser humano-máquina adequadas e suficientemente claras e informativas ;	Art. 20, § 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada , observados os segredos comercial e industrial.
Art. 19, II - transparência quanto às medidas de governança adotadas no desenvolvimento e emprego do sistema de inteligência artificial pela organização;	<p>Art. 49. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares.</p> <p>Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: [...]</p> <p>VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;</p>

Art. 19, III - medidas de gestão de dados adequadas para a **mitigação e prevenção de potenciais vieses discriminatórios**;

Art. 20, §2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para **verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais**.

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes **princípios**: [...]

IX - **não discriminação**: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

Art. 19, V - adoção de **parâmetros adequados de separação e organização dos dados** para treinamento, teste e validação dos resultados do sistema

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes **princípios**: [...]

V - **qualidade dos dados**: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

Art. 19, IV - legitimação do tratamento de dados conforme a legislação de proteção de dados, inclusive por meio da **adoção de medidas de privacidade desde a concepção e por padrão** e da adoção de **técnicas que minimizem o uso de dados pessoais**;

Art. 46. Os agentes de tratamento devem adotar **medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais** de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Art. 19, VI - adoção de **medidas adequadas de segurança da informação desde a concepção** até a operação do sistema

§ 2º As **medidas** de que trata o caput deste artigo deverão ser **observadas desde a fase de concepção do produto ou do serviço até a sua execução**.

§ 1º As medidas de governança dos sistemas de inteligência artificial são aplicáveis ao longo de todo o seu ciclo de vida, **desde a concepção inicial até o encerramento de suas atividades e descontinuação**.

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes **princípios**:

I - **finalidade**: realização do tratamento para propósitos legítimos, específicos, explícitos e

informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - **adequação**: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - **necessidade**: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; [...]

VII - **segurança**: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII - **prevenção**: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

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.

§ 2º Os desenvolvedores e operadores de sistemas de inteligência artificial, poderão:

I – **implementar programa de governança** que, no mínimo:

Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de **boas práticas e de governança** que estabeleçam as **condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos** e outros aspectos relacionados ao tratamento de dados pessoais.

§ 1º Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a **finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes** de tratamento de dados do titular.

§ 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o **controlador**, observados a estrutura, a escala e o volume de suas operações, bem como a

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;

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;

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.

sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, **poderá**:

I – implementar programa de governança em privacidade que, no mínimo:

a) **demonstre o comprometimento do controlador em adotar processos e políticas internas** que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;

b) **seja aplicável a todo o conjunto de dados pessoais** que estejam sob seu controle, independentemente do modo como se realizou sua coleta;

c) **seja adaptado à estrutura, à escala e ao volume de suas operações**, bem como à sensibilidade dos dados tratados;

d) **estabeleça políticas e salvaguardas adequadas** com base em processo de avaliação sistemática de impactos e riscos à privacidade;

e) **tenha o objetivo de estabelecer relação de confiança com o titular**, por meio de atuação transparente e que assegure mecanismos de participação do titular;

f) **esteja integrado a sua estrutura geral de governança** e estabeleça e aplique mecanismos de supervisão internos e externos;

g) **conte com planos de resposta a incidentes e remediação**; e

h) **seja atualizado constantemente** com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;

II – demonstrar a efetividade de seu programa de governança em privacidade quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento desta Lei.

§ 3º A adesão voluntária a código de boas práticas e governança pode ser considerada indicativo de boa-fé por parte do agente e será

Sem correspondência direta.

levada em consideração pela autoridade competente para fins de aplicação de sanções administrativas.	
§ 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.	§ 3º As regras de boas práticas e de governança deverão ser publicadas e atualizadas periodicamente e poderão ser reconhecidas e divulgadas pela autoridade nacional.

Tabela 3: Comparação das competências da autoridade chave do PL nº 2338/2023 com às atribuídas à ANPD pela LGPD

PL nº 2338/2023	LGPD
Art. 13, § 3º A autoridade competente poderá determinar a reclassificação do sistema de inteligência artificial, mediante notificação prévia, bem como determinar a realização de avaliação de impacto algorítmico para instrução da investigação em curso.	Art. 4º, § 3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais . Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais , inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.
Art. 16. Caberá à autoridade competente regulamentar os sistemas de inteligência artificial de risco excessivo .	Art. 55-J: XIII - editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios

gerais de proteção de dados pessoais previstos nesta Lei;

Art. 31. Os agentes de inteligência artificial comunicarão à autoridade competente a ocorrência de graves incidentes de segurança, incluindo quando houver risco à vida e integridade física de pessoas, a interrupção de funcionamento de operações críticas de infraestrutura, graves danos à propriedade ou ao meio ambiente, bem como graves violações aos direitos fundamentais, nos termos do regulamento.

§ 1º A comunicação será feita em **prazo razoável, conforme definido pela autoridade competente**.

§ 2º A **autoridade competente verificará a gravidade do incidente** e poderá, caso necessário, **determinar ao agente a adoção de providências e medidas para reverter ou mitigar os efeitos do incidente**.

Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

§ 1º A comunicação será feita em **prazo razoável, conforme definido pela autoridade nacional**, e deverá mencionar, no mínimo: (...)

§ 2º A **autoridade nacional verificará a gravidade do incidente** e poderá, caso necessário para a salvaguarda dos direitos dos titulares, **determinar ao controlador a adoção de providências**, tais como:

I - ampla divulgação do fato em meios de comunicação; e

II - **medidas para reverter ou mitigar os efeitos do incidente**.

Art. 32, parágrafo único. Cabe à autoridade competente:

I – **zelar pela proteção a direitos fundamentais e a demais direitos afetados** pela utilização de sistemas de inteligência artificial;

Art. 55-J. Compete à ANPD:

I - **zelar pela proteção dos dados pessoais**, nos termos da legislação;

Art. 32, II – promover a elaboração, atualização e implementação da Estratégia Brasileira de Inteligência Artificial junto aos órgãos de competência correlata;

Art. 55-J: III - elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade;

Art. 32, III – **promover e elaborar estudos sobre boas práticas** no desenvolvimento e utilização de sistemas de inteligência artificial;

Art. 55-J: VII - **promover e elaborar estudos sobre as práticas nacionais e internacionais** de proteção de dados pessoais e privacidade;

Art. 32, IV – **estimular a adoção de boas práticas**, inclusive códigos de conduta, no desenvolvimento e utilização de sistemas de inteligência artificial;

Art. 55-J: VIII - **estimular a adoção de padrões** para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis;

Art. 32, 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;**

Art. 55-J: IX - **promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional;**

Art. 32, VI – expedir normas para a regulamentação desta Lei, inclusive sobre:

- a) procedimentos associados ao exercício dos direitos previstos nesta Lei;
- 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
- d) procedimentos para certificação do desenvolvimento e utilização de sistemas de alto risco.

Art. 55-J: X - dispor sobre as formas de publicidade das operações de tratamento de dados pessoais, respeitados os segredos comercial e industrial;

XIII - **editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei;**

Art. 32, VII – **articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação;**

Art. 55-J: XXIII - **articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação;**

Art. 32, 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;

Art. 55-J: IV - **fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação**, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso;

Art. 32, 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;**

Art. 55-J: XI - **solicitar, a qualquer momento, às entidades do poder público que realizem operações de tratamento de dados pessoais 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;**

Art. 32, 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;

Art. 55-J: XVII - **celebrar, a qualquer momento, compromisso com agentes de tratamento 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;

Art. 32, XII – **apreciar petições em face do operador de sistema de inteligência artificial**, após comprovada apresentação de reclamação não solucionada no prazo estabelecido em regulamentação;

Art. 55-J: V - **apreciar petições de titular contra controlador** após comprovada pelo titular a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação;

Art. 35. **Os regulamentos e as normas editados pela autoridade competente serão precedidos de consulta e audiência públicas, bem como de**

Art. 55-J: § 2º **Os regulamentos e as normas editados pela ANPD devem ser precedidos de**

análises de impacto regulatório, nos termos dos arts. 6º a 12 da Lei no 13.848, de 25 de junho de 2019, no que cabível.

consulta e audiência públicas, bem como de análises de impacto regulatório.

Art. 36. Os agentes de inteligência artificial, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes **sanções administrativas aplicáveis pela autoridade competente**:

I – **advertência**;

II – **multa simples**, limitada, no total, a R\$ 50.000.000,00 (cinquenta milhões de reais) por infração, sendo, no caso de pessoa jurídica de direito privado, de até 2% (dois por cento) de seu faturamento, de seu grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos;

III – **publicização da infração** após devidamente apurada e confirmada a sua ocorrência;

IV – proibição ou restrição para participar de regime de sandbox regulatório previsto nesta Lei, por até cinco anos;

V – **suspensão parcial ou total, temporária ou definitiva, do desenvolvimento, fornecimento ou operação do sistema de inteligência artificial**; e

VI – **proibição de tratamento de determinadas bases de dados**

Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes **sanções administrativas aplicáveis pela autoridade nacional**:

I – **advertência**, com indicação de prazo para adoção de medidas corretivas;

II – **multa simples**, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R\$ 50.000.000,00 (cinquenta milhões de reais) por infração;

III – **multa diária**, observado o limite total a que se refere o inciso II;

IV – **publicização da infração** após devidamente apurada e confirmada a sua ocorrência;

V – bloqueio dos dados pessoais a que se refere a infração até a sua regularização;

VI – eliminação dos dados pessoais a que se refere a infração;

X – **suspensão parcial do funcionamento do banco de dados** a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;

XI – **suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração** pelo período máximo de 6 (seis) meses, prorrogável por igual período;

XII – **proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.**

§ 1º As **sanções serão aplicadas após procedimento administrativo** que possibilite a

§ 1º As **sanções serão aplicadas após procedimento administrativo** que possibilite a

oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes **parâmetros e critérios**:

direitos;

I – a **gravidade e a natureza das infrações** e a eventual violação de

II – a **boa-fé do infrator**;

III – a **vantagem auferida ou pretendida pelo infrator**;

IV – a **condição econômica do infrator**;

V – a **reincidência**;

VI – o **grau do dano**;

VII – a **cooperação do infrator**;

VIII – a **adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar riscos**, inclusive a análise de impacto algorítmico e efetiva implementação de código de ética;

IX – a **adoção de política de boas práticas e governança**;

X – a **pronta adoção de medidas corretivas**;

XI – a **proporcionalidade entre a gravidade da falta e a intensidade da sanção**; e

XII – a **cumulação com outras sanções administrativas eventualmente já aplicadas em definitivo para o mesmo ato ilícito**.

oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes **parâmetros e critérios**:

I – a **gravidade e a natureza das infrações** e dos direitos pessoais afetados;

II – a **boa-fé do infrator**;

III – a **vantagem auferida ou pretendida pelo infrator**;

IV – a **condição econômica do infrator**;

V – a **reincidência**;

VI – o **grau do dano**;

VII – a **cooperação do infrator**;

VIII – a **adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano**, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei;

IX – a **adoção de política de boas práticas e governança**;

X – a **pronta adoção de medidas corretivas**; e

XI – a **proporcionalidade entre a gravidade da falta e a intensidade da sanção**.

§ 2º Antes ou durante o processo administrativo do § 1º, poderá a autoridade competente adotar medidas preventivas, incluída multa cominatória, observado o limite total a que se refere o inciso II do caput, quando houver indício ou fundado receio de que o agente de inteligência artificial:

ou

I – cause ou possa causar lesão irreparável ou de difícil reparação;

II – torne ineficaz o resultado final do processo.

Sem correspondência direta.

§ 3º **O disposto neste artigo não substitui a aplicação de sanções administrativas, civis ou penais** definidas na Lei no 8.078, de 11 de setembro de 1990, na Lei no 13.709, de 14 de agosto de 2018, e em legislação específica.

§ 2º **O disposto neste artigo não substitui a aplicação de sanções administrativas, civis ou penais** definidas na Lei nº 8.078, de 11 de setembro de 1990, e em legislação específica.

§ 4º No caso do desenvolvimento, fornecimento ou utilização de sistemas de inteligência artificial de risco excessivo haverá, no mínimo, aplicação de multa e, no caso de pessoa jurídica, a suspensão parcial ou total, provisória ou definitiva de suas atividades.

Sem correspondência direta.

§ 5º A aplicação das sanções previstas neste artigo não exclui, em qualquer hipótese, a obrigação da reparação integral do dano causado, nos termos do art. 27.

Sem correspondência direta.

Art. 37. **A autoridade competente definirá, por meio de regulamento próprio, o procedimento de apuração e critérios de aplicação das sanções administrativas a infrações a esta Lei, que serão objeto de consulta pública**, sem prejuízo das disposições do Decreto-Lei no 4.657, de 4 de setembro de 1942, Lei no 9.784, de 29 de janeiro de 1999, e demais disposições legais pertinentes.

Art. 53. **A autoridade nacional definirá, por meio de regulamento próprio sobre sanções administrativas a infrações a esta Lei, que deverá ser objeto de consulta pública**, as metodologias que orientarão o cálculo do valor-base das sanções de multa. (Vigência)

Parágrafo único. **As metodologias a que se refere o caput deste artigo serão previamente publicadas e apresentarão objetivamente as formas e dosimetrias das sanções**, que conterão fundamentação detalhada de todos os seus elementos, demonstrando a observância dos critérios previstos nesta Lei.

§ 1º **As metodologias a que se refere o caput deste artigo devem ser previamente publicadas, para ciência dos agentes de tratamento, e devem apresentar objetivamente as formas e dosimetrias para o cálculo do valor-base das sanções de multa**, que deverão conter fundamentação detalhada de todos os seus elementos, demonstrando a observância dos critérios previstos nesta Lei.

§ 2º O regulamento de sanções e metodologias correspondentes deve estabelecer as circunstâncias e as condições para a adoção de multa simples ou diária