Comentários do CIPL sobre o Projeto de Lei nº 2338 do Senado Brasileiro

Resumo executivo e contexto relevante para os comentários do CIPL

O Centro de Liderança em Políticas de Informação (CIPL)[1] saúda os autores do Projeto de Lei 2338 por elaborarem uma legislação sobre inteligência artificial (IA) centrada em uma abordagem baseada em riscos e fundamentada em responsabilização organizacional e prestação de contas (*i.e.: accountability)*. O CIPL tem sido um líder em pensamento sobre responsabilidade organizacional e abordagem baseada em risco para políticas e práticas de dados há mais de 20 anos e foi um dos primeiros a contribuir para lidar com desafios de escopo e a definir soluções para a governança em IA e práticas neste setor[2]. O CIPL também preparou respostas detalhadas para consultas públicas sobre políticas de IA no Brasil, na União Europeia, no Reino Unido e nos Estados Unidos[3].

Com base nessa experiência e em nosso amplo envolvimento com líderes do setor privado que desenvolvem e implantam tecnologias de IA, formuladores de políticas e reguladores, em nosso recente documento *Ten Recommendations for Global AI Regulation (Dez Recomendações para uma Regulamentação Global de IA)*, o CIPL oferece recomendações para orientar a formulação de políticas e regulamentação de IA, a fim de permitir uma IA responsável e confiável. O CIPL recomenda uma abordagem baseada em riscos e em níveis para regulamentação da IA que aproveite leis e normas existentes e nas práticas responsáveis das organizações. Essa abordagem deve ser apoiada por supervisão regulatória inovadora e instrumentos de corregulação. Qualquer abordagem legislativa ou regulatória de IA deve seguir estas recomendações abrangentes, que também resumem a visão do CIPL sobre uma abordagem em camadas ou em três níveis para a regulamentação de IA:

A. Regras Baseadas em Princípios e Resultados
   1. Criar uma estrutura flexível e adaptável que defina os resultados a serem atingidos em vez de prescrever detalhes de como atingi-los
   2. Adotar uma abordagem baseada em riscos que considere riscos e benefícios holisticamente.
   3. Basear-se em fundações legais vinculativas e não vinculativas (soft law)
   4. Empoderar indivíduos através de transparência, explicabilidade e mecanismos de compensação

B. Responsabilização Organizacional Demonstrável (i.e.: accountability)
   5. Tornar a responsabilização organizacional demonstrável um elemento central das regulamentações de IA
   6. Promover a adoção de práticas responsáveis de governança em IA
   7. Repartir a responsabilidade cuidadosamente, com foco na parte mais intimamente associada à geração de danos

C. Supervisão Regulamentadora Inteligente

[1] O CIPL é um grupo de reflexão global sobre políticas de privacidade e dados do escritório de advocacia Hunton Andrews Kurth LLP e é apoiado financeiramente por esse escritório de advocacia e por mais de 85 empresas associadas que são líderes em setores-chave da economia global. A missão do CIPL é engajar-se na liderança de pensamento e desenvolver melhores práticas que garantam tanto a proteção efetiva da privacidade quanto o uso responsável de informações pessoais na era moderna da informação. O trabalho do CIPL facilita o engajamento construtivo entre líderes empresariais, profissionais de privacidade e segurança, reguladores e formuladores de políticas em todo o mundo. Para mais informações, consulte o site do CIPL em http://www.informa-tionpolicycentre.com/. Nada neste documento deve ser interpretado como representação de opinião de qualquer empresa membro do CIPL ou do escritório de advocacia de Hunton Andrews Kurth.

[2] As principais contribuições do CIPL nesse campo incluem: *Artificial Intelligence and Data Protection in Tension (Inteligência Artificial e Proteção de Dados em Tensão,* outubro de 2018), *Hard Issues and Practical Solutions (Problemas Difíceis e Soluções Práticas.* fevereiro de 2020), *Artificial Intelligence and Data Protection: How the GDPR Regulates AI* (*Inteligência Artificial e Proteção de Dados: Como a RGPD da UE Regulamenta IA, março de 2020)* e *Ten Recommendations for Global AI Regulation (Dez Recomendações para uma Regulamentação Global de IA, outubro de 2023)*.

[3] CIPL Response to NTIA Request for Comment on AI Accountability Policy (Resposta do CIPL à solicitação da NTIA para comentários sobre política de responsabilização em IA, junho de 2023); CIPL's Top Ten Recommendations for Regulating AI in Brazil (Dez recomendações prioritárias do CIPL para a regulação de IA no Brasil, outubro de 2022); CIPL Response to UK DCMS Proposed Approach to Regulating AI (Resposta do CIPL à abordagem proposta pelo DCMS do Reino Unido para a regulação de IA, setembro de 2022); CIPL Response to the EU Commission's Consultation on the Draft AI Act (Resposta do CIPL à consulta da Comissão da UE sobre projeto de lei de IA), julho de 2021).

8. Criar mecanismos para coordenação e cooperação ao longo dos órgãos regulamentadores
9. Instituir supervisão regulamentadora baseada na cooperação e facilitar inovação regulamentadora contínua
10. Buscar a interoperabilidade global

É encorajador ver essas recomendações adotadas em muitos aspectos do projeto de lei brasileiro. No entanto, identificamos maneiras pelas quais o projeto de lei poderia ser emendado para promover ainda mais responsabilidade organizacional na governança responsável de IA, bem como áreas em que orientações ou esclarecimentos adicionais seriam úteis. A seguir, apresentamos um resumo das principais observações e recomendações do CIPL:

- **Esclarecimento sobre a terminologia** - A minuta do projeto de lei usa alguns conceitos e termos que exigem maior detalhamento para maior clareza. Exemplos notáveis incluem a definição de inteligência artificial; os conceitos de fornecedor, operador e agente de IA; pessoas afetadas por sistemas de IA; o direito à informação prévia com relação a interações com sistemas de IA; e sistemas de reconhecimento de emoções e sistemas de categorização biométrica. O CIPL incentiva a minuta do Projeto de Lei de IA do Brasil a aproveitar marcos consagrados (existentes e emergentes) e suas terminologias consagradas, como as produzidas pela Organização para Cooperação e Desenvolvimento Econômico (OCDE), que podem promover o alinhamento internacional de regulamentações de IA.

- **Abordagem baseada em risco que considere riscos e benefícios de forma holística** - O CIPL apoia a abordagem baseada em risco do projeto de lei de IA do Brasil que atribui obrigações e modelos de governança dependendo do risco associado aos sistemas de IA. Ao fazer isso, em vez de regulamentar a tecnologia em si, o projeto de lei deve regulamentar os riscos que podem resultar em danos indesejados. O CIPL também endossa a abordagem holística, que exige que avaliações de impacto algorítmico incluam tanto riscos mas também benefícios de um determinado sistema de IA.

- **Necessidade de refutabilidade da presunção de risco** - Embora o projeto de lei prescreva uma proibição geral de sistemas de IA que produzam risco excessivo e enumere sistemas de IA de alto risco, o CIPL recomenda que o projeto de lei trate o nível de risco como uma presunção refutável. Isso permitiria que as organizações considerassem a natureza altamente contextual dos aplicativos de IA e lhes daria a oportunidade de demonstrar que o uso de um aplicativo de IA em um contexto específico não apresenta risco excessivo ou alto.

- **Relacionamento com marcos normativos existentes** - O projeto de lei deve evitar duplicar ou criar quaisquer requisitos conflitantes com as marcos normativos existentes, como a LGPD e leis de proteção ao consumidor, antidiscriminação e PI (propriedade intelectual). Embora a linguagem pareça deixar claro que o regulamento de IA é aplicável sem prejuízo da LGPD, seria útil esclarecer quais requisitos do estatuto prevalecem no caso de quaisquer ambiguidades ou conflitos percebidos.

- **Empoderar indivíduos por meio de princípios de IA responsável** - O CIPL apoia a abordagem do projeto de lei para empoderar indivíduos por meio de transparência, explicabilidade e mecanismos de reparação, que serão fundamentais para obtenção de uma IA confiável e benéfica. No entanto, o projeto de lei, ou outras orientações regulatórias, devem esclarecer que os desenvolvedores e implantadores de IA devem oferecer transparência e explicabilidade adequadas ao contexto e significativas sobre as entradas e operações dos sistemas de IA, sem prejuízo de outros objetivos de políticas, como privacidade, segredos comerciais e segurança.

- **Responsabilização organizacional (*accountability*) demonstrável** - O CIPL aplaude o projeto de lei por permitir que agentes de IA formulem códigos de boas práticas e governança e por declarar que a participação em tais mecanismos será vista favoravelmente em ações de aplicação.

- **Abordagem moderna para a supervisão regulatória** - O CIPL endossa a abordagem da minuta do projeto de lei para a criação de um sandbox regulatória com o objetivo de incentivar a inovação em IA. Isso fornecerá espaços seguros supervisionados para que as organizações abordem e resolvam alguns dos aspectos mais desafiadores da implantação de aplicativos de IA, especialmente quando eles parecerem inconsistentes ou em tensão com os requisitos legais vigentes. No entanto, o CIPL está preocupado com a responsabilidade contínua dos participantes no ambiente de teste e recomenda que a participação na sandbox seja tratada como um fator mitigante significativo nas ações de fiscalização se a suposta violação estiver relacionada com atividade que fazia ou faz parte do sandbox.

- **Alocação de responsabilidade** - O ciclo de vida da IA é complexo e envolve diversos atores com responsabilidades variadas ao longo do processo. A lei não deve tratar todos os atores do processo de forma semelhante, pois isso criaria efeitos negativos significativos sobre entidades menores, desenvolvedores de código aberto e inovadores. A minuta do projeto de lei e outras orientações regulatórias devem visar à distribuição adequada da responsabilidade entre as partes do ecossistema de IA, de acordo com sua parcela de responsabilidade pela geração do dano em questão e capacidade de mitigar esse dano. O CIPL

também incentiva o projeto de lei a reconhecer medidas proativas tomadas por organizações de boa-fé como um fator de mitigação em um contexto de aplicação. Isso servirá como um incentivo adicional para que as organizações realizem avaliações de risco.

- **Coordenação e cooperação entre órgãos reguladores** - O CIPL apoia a abordagem do projeto de lei de promover ações cooperativas com autoridades nacionais e internacionais para proteção e promoção do desenvolvimento e uso de sistemas de IA. Essa abordagem seria benéfica tanto para organizações quanto para órgãos reguladores, promovendo a consistência nas abordagens regulatórias, bem como políticas e orientações holísticas e interdisciplinares que são mais fáceis de serem implementadas e monitoradas por órgãos reguladores especializados e pelo setor ao longo do tempo.

- **Confidencialidade das avaliações de impacto algorítmico** - O CIPL está preocupado com a viabilidade e a conveniência de um banco de dados de IA de alto risco previsto no projeto de lei. O acesso a esse banco de dados deve estar sujeito a salvaguardas adequadas para garantir a confidencialidade de dados pessoais, informações comerciais proprietárias e outras informações que possam ser aproveitadas por agentes mal-intencionados para contornarem a finalidade pretendida da IA (por exemplo, uma solução de prevenção de fraudes) ou, por outro lado, para causarem danos. O projeto de lei também poderia afirmar que a divulgação de uma avaliação de impacto algorítmico para a autoridade competente não constitui uma renúncia a qualquer privilégio advogado-cliente ou proteção de produto de trabalho que possa existir com relação a qualquer informação contida nas avaliações de impacto algorítmico.

Por fim, o CIPL gostaria de chamar a atenção para certas iniciativas na arena global na direção do desenvolvimento de princípios e padrões internacionais, refletindo entendimentos e valores compartilhados, obtidos por meio de processos de desenvolvimento com várias partes interessadas. Por exemplo, os Ministros Digitais e de Tecnologia do G7 reafirmaram o papel fundamental dos padrões em sua Cúpula de Hiroshima, em abril de 2023, e os Líderes do G7 anunciaram os Princípios Orientadores Internacionais do Processo de Hiroshima para Organizações que Desenvolvem Sistemas Avançados de IA e, em outubro, o Código de Conduta Internacional do Processo de Hiroshima para Organizações que Desenvolvem Sistemas Avançados de IA. Os ministros do G7 também estão trabalhando para desenvolver uma Estrutura de Política Abrangente, para incluir a cooperação com a Parceria Global em IA (GPAI) e a Organização para Cooperação e Desenvolvimento Econômico (OCDE). O CIPL acredita que a regulamentação brasileira de IA deve considerar as estruturas mencionadas acima para alcançar o alinhamento internacional.

Estamos à disposição para responder a quaisquer perguntas sobre nosso feedback e ajudar ainda mais esse importante esforço legislativo.

Versão PT-EN	COMENTÁRIOS
Art. 1 This Law establishes general rules of a national nature for the development, implementation and responsible use of artificial intelligence (AI) systems in Brazil, with the aim of protecting fundamental rights and guaranteeing the implementation of safe and reliable systems, for the benefit of the human person, the democratic regime and scientific and technological development.	
Art. 2 The development, implementation and use of artificial intelligence systems in Brazil are based on:	• Será importante esclarecer até que ponto os Artigos 2 e 3 devem ser aplicados e, em caso afirmativo, como serão aplicados. • Recomendamos que o padrão para esses princípios seja a capacidade de demonstrar que os atores trabalharam de boa-fé para colocar em prática esses princípios. Tal abordagem permite erros - e a correção desses erros - desde que não tenham sido intencionais ou devidos a imprudência ou negligência. • Além disso, sugerimos que a Lei acrescente o seguinte como base para o "desenvolvimento, implementação e uso de sistemas de IA no Brasil": "XI - A necessidade de considerar e alcançar, quando possível e apropriado, interoperabilidade, convergência ou harmonização global com relação às tecnologias de IA e às políticas e regulamentações aplicáveis."
I – the centrality of the human person;	
II – respect for human rights and democratic values;	
III – the free development of the personality;	
IV – protection of the environment and sustainable development;	
V – equality, non-discrimination, plurality and respect for labor rights;	
VI – technological development and innovation;	
VII – free initiative, free competition and consumer protection;	
VIII – privacy, data protection and informative [sic] [should be informed] self-determination;	
IX – the promotion of research and development with the aim of stimulating innovation in the productive sectors and in public authority;	

X – access to information and education, as well as awareness of artificial intelligence systems and their applications.	
Art. 3 The development, implementation and use of artificial intelligence systems will observe good faith and the following principles:	
I – inclusive growth, sustainable development and well-being;	
II – self-determination and freedom of decision and choice;	
III – human participation in the artificial intelligence cycle and effective human supervision	
IV – non-discrimination;	
V – justice, equity and inclusion;	• É importante esclarecer como justiça, equidade e inclusão serão aferidas na prática e em relação a outras disposições, como a não discriminação (IV) e a autodeterminação e a liberdade de decisão e escolha (II).
VI – transparency, explainability, intelligibility and auditability;	
VII – reliability and robustness of artificial intelligence and information security systems;	• É importante esclarecer como confiabilidade e robustez serão aferidas na prática. Ao mesmo tempo, qualquer orientação sobre isso deve evitar a criação de obrigações prescritivas que sobrecarreguem as organizações desnecessariamente.
VIII – due legal process, contestability and contradictory;	
IX – traceability of decisions during the life cycle of artificial intelligence systems as a means of accountability and attribution of responsibilities to a natural or legal person;	
X – accountability and full compensation for damages;	• É importante criar um ambiente que incentive a inovação e o investimento e, ao mesmo tempo, proteja os consumidores. Para isso, é necessário encontrar um equilíbrio que incentive a inovação responsável. • Deve haver limites para a responsabilidade dos desenvolvedores e provedores de IA por danos se eles tiverem agido de forma responsável ou não tiverem a capacidade de prevenir ou evitar danos decorrentes de outros agentes de IA.

XI – prevention, precaution and mitigation of systemic risks derived from intentional or unintentional uses and unforeseen effects of artificial intelligence systems; and	• Os desenvolvedores e provedores de IA devem ser incentivados a antecipar e mitigar efeitos razoavelmente previsíveis (inclusive o uso indevido razoavelmente previsível) de seus sistemas. No entanto, responsabilizá-los por todos os efeitos, independentemente da dificuldade de previsão, poderia desestimular o investimento e a inovação em sistemas de IA.
XII – non-maleficence and proportionality between the methods employed and the determined and legitimate purposes of artificial intelligence systems.	
Art. 4th. For the purposes of this Law, the following definitions are adopted:	
I – artificial intelligence system: computational system, with different degrees of autonomy, designed to infer how to achieve a given set of objectives, using approaches based on machine learning and/or logic and knowledge representation, through input data from machines or humans, with the aim of producing predictions, recommendations or decisions that may influence the virtual or real environment.	• É importante que o projeto de lei forneça uma definição de IA que seja idêntica ou interoperável com as definições padrão emergentes no plano global, como a desenvolvida pela Organização para Cooperação e Desenvolvimento Econômico (OCDE): "*Um sistema de IA é um sistema baseado em máquina que, para objetivos explícitos ou implícitos, infere, a partir de entradas que recebe, como gerar resultados - tais como previsões, recomendações ou decisões - que podem influenciar ambientes físicos ou virtuais. Diferentes sistemas de IA variam em seus níveis de autonomia e adaptabilidade após a implantação.*" • A definição atual de IA no projeto de lei é excessivamente ampla, correndo o risco de aplicar-se a praticamente todos os tipos de software, em vez de visar os riscos específicos que a Lei pretende abordar. Em particular, a formulação atual não inclui apenas "abordagens de aprendizado de máquina" de vários tipos, mas também inclui toda "lógica e representação de conhecimento". Isso poderia incluir praticamente qualquer software computadorizado, mesmo aqueles que não apresentam os riscos que a Lei tenta abordar. Para garantir uma aplicação consistente, o elemento de geração de resultados (previsões, recomendações ou decisões) da definição deve ser delimitado de forma a abranger os resultados de IA gerados pelo sistema, ou seja, sistemas de IA cujos resultados são gerados com base em regras decorrentes do próprio sistema de IA, e não gerados por humanos, tal como uma planilha sofisticada de Excel, cuja lógica é totalmente desenvolvida e controlada por humanos.

II – supplier of an artificial intelligence system: natural or legal person, whether public or private, who develops an artificial intelligence system, directly or by order, with a view to placing it on the market or using it in the service provided by it, under its own name or brand, for a fee or free of charge;	• Comentários sobre II, III e IV:
	
	• A tipologia dos atores de IA no projeto de lei apresenta algumas semelhanças, mas também diferenças importantes em relação às estruturas regulatórias em outras jurisdições. O Brasil pode querer considerar como essas convergências e divergências podem afetar a interoperabilidade da legislação brasileira com leis de outras jurisdições. O Brasil pode considerar a possibilidade de alavancar estruturas de leis não vinculativas, como a taxonomia de atores da IA da UNCITRAL, que pode promover o alinhamento internacional das regulamentações de IA. Assim, usando as recomendações da OCDE como base, a UNCITRAL divide os atores envolvidos em sistemas de IA em quatro categorias amplas, a saber:
	
	  ◦ "(a) *desenvolvedor*: pessoa responsável pelo projeto teórico de alto nível, programação, treinamento e verificação do sistema de IA e pela interface e integração com hardware, aplicativos e fontes de dados externos, antes da implantação;
	
	  ◦ (b) *provedor de dados*: pessoa que fornece - ou é responsável por fornecer - dados ao sistema (ou seja, os dados necessários para apoiar o treinamento, a implantação ou a operação);
	
	  ◦ (c) *implantador*: a pessoa que implanta o sistema, integrando-o a suas operações (por exemplo, os

	bens e serviços que fornece), inclusive configurando, gerenciando, mantendo e apoiando o fornecimento de dados e a infraestrutura necessários para operação e monitoramento do sistema de IA e sua interação com os dados fornecidos, uma vez implantados;
	
	• (d) *operador*: a pessoa que opera o sistema:
	
	  • (i) em muitos casos, o operador será a pessoa que implementa o sistema;
	  • (ii) em alguns casos, o operador pode ser o usuário final de bens ou serviços habilitados para IA (por exemplo, se o usuário final tiver algum controle sobre a operação dos bens ou serviços);
	
	• (e) *pessoa afetada*: qualquer outra pessoa afetada pela operação de um sistema de IA, inclusive por interagir com o sistema (por exemplo, fornecendo dados ao sistema) ou por ser o usuário final de bens ou serviços habilitados para IA."
	
	• Há questões importantes que precisarão ser esclarecidas com relação aos limites de cada definição e onde exemplos específicos se enquadrariam. Por exemplo, se uma entidade adquire um sistema de IA de uso geral e depois personaliza os recursos nele contidos antes da implementação, ela será tratada como fornecedor?
	
	• O termo "fornecedor" é usado de forma intercambiável com "provedor" neste projeto de lei?

III – operator of an artificial intelligence system: natural or legal person, whether public or private, who employs or uses, in its name or benefit, an artificial intelligence system, unless said system is used within the scope of a personal activity of unprofessional character.	• Veja acima (Artigo 4/II).
IV – artificial intelligence agents: providers and operators of artificial intelligence systems.	• Veja os comentários acima (Artigo 4/II) - "agentes" aqui parece estar próximo da função de "operadores", de acordo com a Lei de IA da UE. Orientações podem ajudar a esclarecer melhor este ponto.
V – competent authority: body or entity of the Federal Public Administration responsible for ensuring, implementing and supervising compliance with this Law throughout the national territory;	
VI – discrimination: any distinction, exclusion, restriction or preference, in any area of public or private life, which purpose or effect is to annul or restrict the recognition, enjoyment or exercise, under conditions of equality, of one or more rights or freedoms provided for in the legal system, due to personal characteristics such as geographic origin, race, color or ethnicity, gender, sexual orientation, socioeconomic class, age, disability, religion or political opinions.	• Comentário sobre VI e VII: Discriminação e discriminação indireta são conceitos importantes - é preciso garantir que esses conceitos sejam consistentes aqui com a forma como eles podem ser definidos em outras partes da legislação brasileira, por exemplo, o Estatuto da Igualdade Racial, para garantir proteções consistentes.
VII – indirect discrimination: discrimination that occurs when an apparently neutral rule, practice or criterion has the capacity to bring disadvantage to people belonging to a specific group, or puts them at a disadvantage, unless that rule, practice or criterion has some objective or reasonable justification and legitimate in light of the right to equality and other fundamental rights;	
VIII - text and data mining: process of extracting and analyzing large amounts of data or partial or full excerpts of textual	

content, from which patterns and correlations are extracted that will generate relevant information for the development or use of artificial intelligence systems.	
Art. 5 People affected by artificial intelligence systems have the following rights, to be exercised in the manner and under the conditions described in this Chapter:	• O conceito de "pessoas afetadas por sistemas de IA" precisa ser mais bem delimitado, a menos que tenha um significado específico em outra legislação ou jurisprudência. O conceito fornece uma lista de direitos; portanto, é importante fornecer esclarecimentos e segurança jurídica sobre o texto. Caso contrário, é provável que se dirija a todos de maneira indistinta. Além disso, o Projeto de Lei não prescreve limites jurisdicionais nem exige que os indivíduos tenham um vínculo específico com o Brasil. É necessário esclarecer se tal nexo será exigido para que os indivíduos sejam cobertos pela lei. • O Artigo 20 da LGPD especifica que uma "pessoa afetada" com relação a uma tomada de decisão automatizada é alguém que está (a) sujeito a uma decisão tomada exclusivamente por meio do processamento automatizado de dados pessoais ~~por um sistema de IA~~; (b) quando essa decisão afeta seu perfil pessoal, profissional, de consumo e de crédito, ou aspectos de sua personalidade. Se o conceito de "afetado" for mais amplo do que as condições especificadas na LGPD, uma orientação adicional poderia ajudar a oferecer segurança jurídica.
I – right to prior information regarding their interactions with artificial intelligence systems;	• "Interação" pode precisar de mais especificações para maior clareza. A intenção é abranger todas as circunstâncias em que os indivíduos interagem ativamente com um sistema de IA ou também abrangeria circunstâncias em que os dados de um indivíduo são processados por um sistema de IA sem interação ativa do indivíduo? • Orientações ou regras adicionais serão úteis para se indicar claramente que tipos de informações devem ser compartilhadas com indivíduos. Deve haver um esforço para fornecer a eles informações que sejam úteis e não tão excessivas a ponto de levar à "fadiga da notificação". As informações devem ser oferecidas considerando-se cuidadosamente a capacidade dos consumidores quanto ao entendimento das informações oferecidas, avaliação de consequências e tomada de decisões com base nisso. Essas obrigações de transparência devem ser consistentes com aquelas exigidas pela LGPD. • Aplicar os princípios de uma abordagem baseada em riscos é vital: informações devem ser oferecidas para se tratar dos riscos aos direitos fundamentais dos indivíduos, de forma e na medida em que sejam úteis e acionáveis.
II – right to an explanation about the decision, recommendation or predictions made by artificial intelligence systems;	• Explicabilidade e transparência devem ser equilibradas com outros objetivos de políticas (por exemplo, direitos de propriedade intelectual, marca registrada, segurança do código-fonte etc.). O diálogo ainda está em andamento na comunidade de IA quanto à melhor forma de se promover explicabilidade de IA e aumentar a transparência significativa. A Lei também deve esclarecer a relação da disposição com o Artigo 20(1) da LGPD, que prescreve que o controlador deve fornecer, sempre que solicitado, informações claras e adequadas sobre os critérios e procedimentos utilizados para a decisão automatizada, em conformidade com segredos comerciais e industriais. • O escopo da divulgação precisa ser esclarecido – veja-se, por exemplo, a orientação preparada pelo ICO do Reino Unido sobre explicabilidade de IA. Uma divulgação excessivamente ampla pode fazer com que agentes mal-intencionados acessem informações para fins inadequados e pode não ser compreendida pelos indivíduos se for oferecida em formato excessivamente técnico. Deve-se exigir que as organizações

	encontrem maneiras simples de informar indivíduos sobre a lógica subjacente ou os critérios usados para se chegar à decisão sem oferecer uma explicação complexa dos algoritmos usados em circunstâncias em que essa divulgação provavelmente não será útil; embora devam existir caminhos para que reguladores e pesquisadores acessem essas informações em circunstâncias adequadas. ● O oferecimento de transparência adequada é contextual e as regras sobre transparência devem ser flexíveis o suficiente para acomodar diferentes casos de uso. A Lei não deve se referir a apenas uma abordagem para explicar decisões tomadas com ajuda de IA ou para oferecer um único tipo de informação aos indivíduos afetados. Em vez disso, o contexto afeta o tipo de explicação que as organizações usam para tornar uma decisão assistida por IA clara ou fácil para os indivíduos entenderem. ● A linguagem existente significa que os indivíduos afetados podem invocar esse direito para qualquer sistema de IA; entretanto, de acordo com a abordagem baseada em risco, isso só deve ser aplicável a casos de uso de alto risco. ● O conceito de "decisão" requer esclarecimento sobre quais atividades estarão dentro do escopo.
III – right to challenge decisions or predictions of artificial intelligence systems that produce legal effects or that significantly impact the interests of the affected party;	● Embora os efeitos legais sejam relativamente fáceis de serem identificados, é importante que as autoridades ofereçam exemplos de decisões automatizadas que produzam efeitos significativos.
IV – right to determination and human participation in decisions of artificial intelligence systems, taking into account the context and the state of the art of technological development;	● A abordagem da Lei para considerar o estado da arte e o contexto é positiva; no entanto, o direito à participação humana deve ser estruturado dentro de uma abordagem baseada em risco que associe o direito de se solicitar revisão pós-processamento - e reparação no caso de um dano ser identificado - com uma avaliação de risco *ex-ante* e medidas robustas para se mitigar o risco de possíveis danos.
V – right to non-discrimination and correction of direct, indirect, illegal or abusive discriminatory biases; and	● A Lei deve incluir uma linguagem que enfatize que ela pretende limitar apenas a discriminação ilícita/abusiva e prejudicial.
VI – the right to privacy and protection of personal data, under the terms of the relevant legislation.	● Essa linguagem parece deixar claro que a regulamentação de IA é aplicável sem prejuízo da LGPD. Seria útil esclarecer quais requisitos do estatuto prevalecem no caso de haver ambiguidades ou conflitos percebidos.
Sole paragraph. Artificial intelligence agents will inform, in a clear and easily accessible way, the procedures necessary for the exercise of these rights.	● O agente é definido como provedores e operadores do sistema de IA. Seria útil um texto legislativo adicional, ou uma orientação complementar, para esclarecer os limites das responsabilidades de provedores comparativamente às de operadores.
Art. 6 The defense of the interests and rights provided for in this Law may be exercised before the competent administrative bodies, as well as in court, individually or collectively, in accordance with the provisions of the relevant legislation regarding individual, collective and diffuse protection instruments.	● Conforme observado acima, o Projeto de Lei define "pessoas afetadas por sistemas de IA" de forma ampla (Artigo 5) e parece dar a qualquer pessoa, inclusive àquelas que não têm conexão ou vínculo específico com o Brasil, o direito de invocar os interesses e direitos previstos nesta Lei. Seria útil esclarecer se esse é o escopo de aplicação pretendido.
Rights associated with information and understanding of decisions made by artificial intelligence systems	
Art. 7 People affected by artificial intelligence systems have the right to receive, prior to contracting or using the artificial	● Conforme observado acima, o conceito de "pessoas afetadas por sistemas de IA" precisa ser esclarecido, a menos que tenha um significado específico na ordem jurídica do Brasil.

intelligence system, clear and adequate information regarding the following aspects:	• Seria útil esclarecer as funções e responsabilidades dos provedores em relação aos operadores (ou outros atores de IA ao longo do ciclo de vida) para fornecer essas informações, a fim se de evitar possíveis duplicações ou falta de conformidade. • A Lei deve reconhecer que o significado de transparência efetiva no contexto de IA depende da natureza do público-alvo, o qual informará o nível e o tipo de informação a ser fornecida.
I – automated character of the interaction and decision in processes or products that affect the person;	
II – general description of the system, types of decisions, recommendations or predictions that it is intended to make and consequences of its use for the person;	
III – identification of the operators of the artificial intelligence system and governance measures adopted in the development and use of the system by the organization;	
IV – role of the artificial intelligence system and the humans involved in the decision-making, forecasting or recommendation process;	
V – categories of personal data used in the context of the functioning of the artificial intelligence system;	
VI – security, non-discrimination and reliability measures adopted, including accuracy, precision and coverage; and	• A transparência das medidas de segurança deve ser devidamente equilibrada com os imperativos de segredo comercial, bem como com os riscos de segurança que poderiam ser consequência da revelação de demasiados detalhes sobre a operação de mecanismos de segurança a agentes mal-intencionados. • O significado de "cobertura" deve ser esclarecido.
VII – other information defined in regulation.	
Paragraph 1 Without prejudice to the provision of complete information in a physical or digital medium open to the public, the information referred to in item I of the head of this article will also be provided, when appropriate, with the use of easily recognizable icons or symbols.	
Paragraph 2 Persons exposed to emotion recognition systems or biometric categorization systems will be informed about the use and functioning of the system in the environment where exposure occurs.	• "Sistemas de reconhecimento de emoções" e "sistemas de categorização biométrica" devem ser claramente delimitados e devem estar alinhados com as proteções existentes da LGPD para dados pessoais sensíveis. É importante observar que há um debate ativo internacionalmente sobre quais sistemas devem e quais não devem estar dentro do escopo das regulamentações para sistemas biométricos; será importante que a lei ofereça clareza sobre as disposições relevantes dessa lei.

Paragraph 3 The artificial intelligence systems that are intended for vulnerable groups, such as children, adolescents, the elderly and people with disabilities, will be developed in such a way that these people are able to understand their functioning and their rights vis-à-vis artificial intelligence agents.	• A Lei deve esclarecer o conceito de "grupo vulnerável". A intenção é ser consistente com a LGPD (por exemplo, Art. 14 da LGPD - processamento de dados pessoais de crianças e adolescentes)? • Pode ser útil qualificar o requisito com "na medida do possível" para permitir a prestação de serviços em algumas circunstâncias em que pode não ser possível assegurar tal entendimento (por exemplo, para indivíduos muito jovens ou idosos e enfermos) e onde representantes legais podem ser capazes de agir em nome deles.
Art. 8 The person affected by an artificial intelligence system may request an explanation of the decision, predictions or recommendation, with information regarding the criteria and procedures used, as well as the main factors that affect such specific predictions or decision, including information on:	• A Lei deve incentivar as organizações a desenvolverem práticas recomendadas de explicabilidade e transparência de IA, como parte da prestação de contas e do desenvolvimento e uso responsável e ético da tecnologia. • A Lei deve evitar a prescrição de direitos de acesso de modo que venha a exigir das organizações o fornecimento de descrições demasiadamente detalhadas de algoritmos complexos por trás de processos automatizados de tomada de decisão. Isso é particularmente importante para garantir que as empresas possam oferecer informações significativas aos consumidores comuns sobre as decisões automatizadas subjacentes e sua lógica. A transparência total dos algoritmos (ou seja, a divulgação do código-fonte ou de descrições extensas do funcionamento interno dos algoritmos) não é significativa para usuários e não os faz entender melhor como seus dados estão sendo tratados nos processos automatizados de decisão. • Os direitos de transparência e explicabilidade devem ser equilibrados com os interesses legítimos das empresas em proteger seus segredos comerciais e tipos semelhantes de informações, por exemplo, direitos de propriedade intelectual, que seriam colocados em risco por meio de exigências detalhadas de divulgação. • A abrangência dos sistemas de IA é tal que a imposição de obrigações de transparência e explicabilidade a todos eles não seria impactante ou mesmo significativa para o usuário. Em vez disso, de acordo com a abordagem baseada em risco que deveria estar sustentando a legislação de IA, esses requisitos devem se aplicar aos sistemas de IA classificados como tendo maior risco de danos e não a cada aplicativo individual.
I – the rationality and logic of the system, as well as the meaning and expected consequences of such a decision for the affected person;	• As organizações devem ter a flexibilidade de ponderar esse requisito em relação a seus interesses legítimos, tal como direitos de propriedade intelectual. Além disso, pode não ser tecnicamente possível sempre descrever a lógica do sistema; portanto, a Lei deve incluir a linguagem flexível de "sempre que possível e apropriado". • As regras sobre explicabilidade devem oferecer relevância para a pessoa afetada. A complexidade de alguns sistemas de IA pode tornar inviável o fornecimento de informações detalhadas sobre cada parâmetro e instrução usados para orientar a tomada de decisões de forma compreensível e útil para um usuário final.
II – the degree and level of contribution of the artificial intelligence system to decision-making;	
III – the data processed and its source, as well as the criteria for decision-making and, where appropriate, their weighting, applied to the situation of the affected person;	• Exigir a divulgação de conjuntos completos de dados pode sobrecarregar os usuários com grandes quantidades de informações que podem não ser úteis, além de criar riscos à privacidade e ao segredo comercial. • É importante que sejam oferecidas informações que sejam contextualmente valiosas para as pessoas afetadas e, ao mesmo tempo, que sejam preservados os incentivos para que as empresas criem e mantenham conjuntos de dados e permitir que elas se protejam contra riscos à privacidade e outros danos que possam resultar da divulgação inadequada de dados.

IV – the mechanisms through which the person can challenge the decision; and	
V – the possibility of requesting human intervention, under the terms of this law.	
Sole Paragraph. The information mentioned in the main sentence will be provided by a free and facilitated procedure, in language that allows the person to understand the result of the decision or prediction in question, within a period of up to fifteen days from the request, allowing the extension, once, for equal period, depending on the complexity of the case.	• Seria útil uma orientação sobre como se oferecer divulgações amigáveis e de fácil entendimento ao usuário. Essa orientação também deve avaliar a eficácia e o valor das divulgações de IA no contexto de outras divulgações existentes ao consumidor para se reduzir confusão ou sobrecarga de informações.
The right to challenge decisions and request human intervention	
Art. 9 The person affected by an artificial intelligence system will have the right to contest and request the review of decisions, recommendations or predictions generated by such a system that produce relevant legal effects or that significantly impact their interests.	• A Lei deve oferecer exemplos ilustrativos de efeitos e parâmetros legais igualmente significativos para que o limiar previsto no artigo seja atingido. Se o direito de contestação de decisões e solicitação de revisão se aplicar a cenários de baixo risco e estiver desconectado de ameaças a direitos fundamentais, corre-se o risco de criar uma obrigação que os provedores podem ter dificuldade de cumprir, considerando o número potencial de usuários e solicitações que poderiam se materializar.
Paragraph 1 The right to correct incomplete, inaccurate or outdated data used by artificial intelligence systems is assured, as well as the right to request the anonymization, blocking or elimination of unnecessary, excessive or data processed in violation of the legislation, under the terms of the art. 18 of Law No. 13,709, of August 14, 2018 and the relevant legislation.	• Isso pode não ser possível em todos os sistemas e casos de uso. Sugerimos acrescentar "quando tecnicamente possível".
Paragraph 2 The right to challenge provided for in the main sentence of this article also covers decisions, recommendations or predictions supported by discriminatory, unreasonable inferences or that violate objective good faith, thus understood inferences that:	
I – are based on inadequate or abusive data for the purposes of the processing;	• A definição de "dados abusivos" deve ser esclarecida.
II – are based on imprecise or statistically unreliable methods; or	• Algumas tecnologias, metodologias e métodos amadurecem com o tempo. Precisão e confiabilidade são incrementais e não está claro quais limites serão considerados razoáveis.
III – do not adequately consider the individuality and personal characteristics of individuals.	• Seria útil uma orientação adicional sobre a definição desses termos e seu efeito pretendido.
Art. 10. When the decision, prediction or recommendation of an artificial intelligence system produces relevant legal effects or that significantly impacts the interests of the person, including through the generation of profiles and the making of inferences, the person may request human intervention or review.	• Encargos mais altos devem ser limitados a sistemas de IA de alto risco, que produzem efeitos legais ou igualmente significativos sobre indivíduos. No entanto, esta disposição requer uma delimitação mais precisa, pois pode tratar de sistemas de IA que produzem pouco ou nenhum efeito significativo sobre os indivíduos, como a criação de perfis em contextos de menor risco, e obriga as organizações a oferecer intervenção humana em conformidade.

Sole Paragraph. Human intervention or review will not be required if its implementation proves to be impossible, in which case the person responsible for operating the artificial intelligence system will implement effective alternative measures, in order to ensure the reanalysis of the contested decision, taking into account the arguments raised by the affected person, as well as repairing any damage caused.	• As exigências de correção devem ser proporcionais ao risco potencial do sistema. Conforme a redação atual desta cláusula, mesmo um sistema de baixo risco que não possa oferecer revisão humana seria obrigado a fornecer uma reanálise, independentemente do ônus ou do benefício que ela proporcionaria.
Art. 11. In scenarios in which decisions, predictions or recommendations generated by artificial intelligence systems have an irreversible impact or are difficult to reverse or involve decisions that may pose risks to the life or physical integrity of individuals, there will be significant human involvement in the decision-making process and ultimate human determination.	• A orientação regulamentar subsequente deve fornecer uma lista de exemplos ilustrativos e critérios sobre o que constitui um impacto irreversível. • Nem todas as decisões que são irreversíveis representam riscos significativos para os indivíduos. De fato, muitos sistemas de IA produzem resultados os quais não faz sentido se reverter, justamente por serem de baixo risco. Nesses casos de baixo risco, não é necessário exigir determinações humanas finais.
The right to non-discrimination and correction of direct, indirect, illegal or abusive discriminatory biases	
Art. 12. People affected by decisions, predictions or recommendations of artificial intelligence systems are entitled to fair and isonomic treatment, with the implementation and use of artificial intelligence systems that may lead to direct, indirect, illegal or abusive discrimination being prohibited, including:	• Muitas vezes, é necessário processar formas sensíveis de informações pessoais (por exemplo, dados sobre raça, etnia, gênero etc.) para evitar e detectar vieses em algoritmos. Pode ser útil esclarecer que o processamento de dados de pessoais sensíveis é permitido com ou sem o consentimento do titular dos dados para a garantia de que essas obrigações sejam cumpridas, de acordo com o Artigo 11 (2) (a) da LGPD, que permite que os controladores processem dados sensíveis para garantir o cumprimento de uma obrigação legal.
I – as a result of the use of sensitive personal data or disproportionate impacts due to personal characteristics such as geographic origin, race, color or ethnicity, gender, sexual orientation, socioeconomic class, age, disability, religion or political opinions; or	• Conforme observado acima, muitas vezes é necessário que formas confidenciais de informações pessoais sejam processadas para se evitar e detectar vieses em algoritmos. • Isso está de acordo com a proposta da Lei de IA da UE, que permite o processamento de dados confidenciais de acordo com o RGPD, na medida em que isso seja estritamente necessário para se garantir o monitoramento, a detecção e a correção de viés em relação a sistemas de IA de alto risco, sujeito a salvaguardas adequadas. • Uma avaliação de risco adequada pode determinar o uso apropriado de dados confidenciais para identificar e abordar resultados inadequados e tendenciosos. • Ao mesmo tempo, é importante observar que alguns dados não classificados como "sensíveis", de acordo com a legislação existente, ainda podem estar associados a riscos mais altos. Por exemplo, embora o Artigo 5(II) da LGPD não classifique gênero como dado sensível, os dados que indicam o gênero de uma pessoa podem representar riscos maiores, que podem exigir proteções e mitigações proporcionais.
II – due to the establishment of disadvantages or aggravation of the situation of vulnerability of people belonging to a specific group, even if apparently neutral criteria are used.	
Sole Paragraph. The prohibition provided for in the main sentence does not prevent the adoption of criteria for differentiating between individuals or groups when such differentiation is based on demonstrated, reasonable and legitimate objectives or justifications in light of the right to equality and other fundamental rights.	

RISK CATEGORIZATION	
Preliminary Assessment	
Art. 13. Before being placed on the market or used in service, every artificial intelligence system will undergo a preliminary assessment carried out by the supplier to classify its degree of risk, whose registration will consider the criteria provided for in this chapter.	• Não está claro que "registro" é referido aqui. • O requisito de avaliação preliminar aborda apenas fornecedores, mas não operadores. Parece pressupor que operadores só usarão sistemas de IA em configurações ou para fins compatíveis com os especificados pelo fornecedor. Seria útil observar que o uso fora dessas especificações poderia introduzir riscos diferentes, que exigiriam avaliação adicional. • Para maior clareza, deve ser especificado que a avaliação preliminar consistirá em uma simples pré-triagem ou avaliação de triagem para determinar se uma avaliação de impacto em grande escala é necessária, considerando os critérios fornecidos na lei e na orientação. Isso permitiria que as organizações alocassem melhor seus recursos para a avaliação de aplicativos de IA que podem apresentar alto risco e evitaria que as organizações realizassem a avaliação do uso de IA em contextos em que é óbvio que há muito pouco risco envolvido. • Qualquer exigência de consulta prévia aos órgãos reguladores ou avaliações prévias de conformidade deve ser limitada apenas aos usos de IA de alto risco em que os riscos não possam ser suficientemente mitigados e os riscos residuais permaneçam altos. • O regulamento, ou a orientação regulatória de acordo com o regulamento, deve fornecer critérios ilustrativos às organizações para determinação dos níveis/classificações de risco, especialmente na determinação de aplicações de IA de alto risco.
Paragraph 1 The suppliers of general-purpose artificial intelligence systems shall include in their preliminary assessment the purposes or applications indicated, pursuant to art. 17 of this law.	• Para os fornecedores, seria impossível documentar cada uso concebível de um sistema de IA. Em vez disso, a disposição deve garantir que os fornecedores documentem claramente os principais usos pretendidos do sistema.
Paragraph 2 There will be a record and documentation of the preliminary assessment carried out by the supplier for the purposes of accountability in case the artificial intelligence system is not classified as high risk.	
Paragraph 3 The competent authority may determine the reclassification of the artificial intelligence system, upon prior notification, as well as determine the carrying out of an algorithmic impact assessment to instruct the ongoing investigation.	
Paragraph 4 If the result of the reclassification identifies the artificial intelligence system as high risk, carrying out an algorithmic impact assessment and adopting the other governance measures provided for in Chapter IV will be mandatory, without prejudice to any penalties in the case of a preliminary assessment fraudulent, incomplete or untrue.	
Excessive Risk	

Art. 14. It is prohibited the implementation and use of artificial intelligence systems:	• Recomendamos a criação de uma lista de usos que são "presumivelmente proibidos". Organizações que ainda quiserem se envolver nesses usos precisarão mitigar riscos e obter aprovação da autoridade relevante, sujeita a um padrão de prova adequadamente robusto de que os benefícios para os indivíduos ou para a sociedade superam substancialmente os riscos mitigados. • Seria útil uma orientação mais detalhada, incluindo exemplos, sobre as atividades proibidas.
I – that employ subliminal techniques that have the purpose or effect of inducing the natural person to behave in a way that is harmful or dangerous to their health or safety or against the foundations of this law;	• As proibições não devem ser usadas levianamente e devem ser cuidadosamente limitadas a categorias claramente identificadas. As "técnicas subliminares" não estão definidas e demandam mais clareza para serem incluídas.
II – that exploit any vulnerabilities of specific groups of natural persons, such as those associated with their age or physical or mental disability, in order to induce them to behave in a way that is harmful to their health or safety or against the foundations of this law;	• A disposição em questão é imprecisa com relação ao termo "vulnerabilidades de grupos específicos de pessoas físicas"; não está claro se os exemplos fornecidos pretendem ser exaustivos ou meramente ilustrativos.
III – by the government, to evaluate, classify or rank natural persons, based on their social behavior or personality attributes, through universal scoring, for access to goods and services and public policies, illegitimately or disproportionate.	
Art. 15. Within the scope of public security activities, the use of remote biometric identification systems on a continuous basis in spaces accessible to the public is only permitted, when provided for in specific federal law and judicial authorization in connection with the activity of individualized criminal prosecution, in the following cases:	
I – prosecution of crimes punishable by a maximum sentence of imprisonment of more than two years;	
II – search for victims of crimes or missing persons;	
III – ongoing crime.	
Sole Paragraph. The law referred to in the main sentence shall provide for proportionate and strictly necessary measures to serve the public interest, subject to due legal process and judicial control, as well as the principles and rights provided for in this Law, especially the guarantee against discrimination and the need to review of the algorithmic inference by the public official in charge before taking any action against the identified person.	
Art. 16. It will be up to the competent authority to regulate excessively risky artificial intelligence systems.	• Isso exige orientação/clareza regulatória imediata para que as organizações evitem inseguranças jurídicas. Uma abordagem mais adequada seria (i) descrever fatores, critérios e possíveis danos que as avaliações de risco devem considerar; (ii) fornecer, no máximo, uma lista ilustrativa de usos de risco potencialmente excessivos que podem ser refutados em cada caso; (iii) fornecer orientação contínua sobre como avaliar riscos e benefícios com base no aprendizado ao longo do tempo.
High Risk	

Art. 17. High-risk artificial intelligence systems are those used for the following purposes:	• A criação de listas predeterminadas e categóricas de quais tipos de atividades de processamento são sempre de alto risco resultaria tanto em regulamentação excessiva, impedindo assim atividades de processamento benéficas que podem não justificar o tratamento de alto risco em um determinado contexto, quanto em regulamentação insuficiente, impedindo mitigações eficazes onde o tratamento de alto risco seria justificado. • A estrutura para identificar aplicativos de IA de alto risco cobertos deve envolver o uso de avaliações de impacto projetadas para avaliar a probabilidade, a gravidade e a escala do impacto do uso de IA. • A abordagem para identificar aplicativos de IA de "alto risco" cobertos deve funcionar para organizações de todos os tamanhos. Ela não deve ser muito complexa, prescritiva ou de múltiplas camadas, o que seria desproporcional para a maioria das organizações, difícil de se aplicar na prática e poderia prejudicar o desenvolvimento e a implantação de tecnologias inovadoras de IA. • As ilustrações de aplicativos de IA de alto risco fornecidas no regulamento ou na orientação regulatória devem ser tratadas como presunções refutáveis. Isso permitiria que as organizações levassem em conta a natureza altamente contextual dos aplicativos de IA e lhes daria a oportunidade de demonstrar que o uso de um aplicativo de IA em um contexto específico não apresenta alto risco. Essa abordagem, por exemplo, pode ser observada no mandato de negociação do Parlamento Europeu em relação à Lei de IA da UE, segundo o qual os fornecedores de determinados sistemas de IA podem refutar a presunção de que o sistema deva ser considerado um sistema de IA de alto risco. • Em alguns casos, os benefícios de um uso de IA para indivíduos ou grupo de indivíduos podem ser significativos, apesar de seus riscos. Embora o benefício do uso de IA não deva afetar diretamente a classificação de risco de um aplicativo de IA, a consideração do benefício reduziria o risco de reticência de não se levar adiante o aplicativo de IA benéfico pretendido apenas devido à possibilidade de alto risco. Uma ponderação entre benefícios e riscos poderia ser executada. No contexto de IA, isso exige que uma organização pondere os interesses legítimos do uso de uma tecnologia de IA (para a organização, indivíduos, grupos de indivíduos, sociedade) em relação aos interesses ou direitos fundamentais dos indivíduos de modo a garantir que tanto os benefícios quanto os riscos sejam considerados e ponderados entre si no desenvolvimento e na implementação de um determinado aplicativo de IA.
I – application as safety devices in the management and operation of critical infrastructures, such as traffic control and water and electricity supply networks;	• O conceito de "infraestrutura crítica" precisa ser delimitado, a menos que haja um significado específico na estrutura legal do Brasil. Também não está claro se os exemplos fornecidos têm a intenção de ser exaustivos ou meramente ilustrativos.
II – professional education and training, including systems for determining access to education and professional training institutions or for evaluating and monitoring students;	
III – recruiting, sorting, filtering, evaluating candidates, making decisions about promotions or termination of contractual employment relationships, task sharing and control and evaluation of the performance and behavior of people affected by such artificial intelligence applications in employment areas , worker management and access to self-employment;	• Conforme mencionado acima, a Lei deve considerar que o nível de risco de um sistema de IA depende das circunstâncias específicas do caso de uso de IA. Por exemplo, a IA usada para recrutamento pode ser sensível, mas pode haver casos de uso de recrutamento em que o risco é baixo porque não há impacto considerável nas perspectivas de carreira e nos meios de subsistência futuros. Da mesma forma, a IA usada para alocação de tarefas pode ser sensível quando é usada para determinar as principais atividades profissionais de um funcionário, o que pode afetar as oportunidades de desenvolvimento futuro desse funcionário. No entanto, há situações em que o uso de IA para alocação de tarefas não apresenta nenhum dos mesmos riscos. Por exemplo, uma organização pode optar por usar um sistema de alocação de tarefas baseado em IA para distribuir tarefas entre um grupo de voluntários para atribuições de curto prazo (por exemplo, em outro

	departamento ou região), além de seu trabalho diário, com base nas respectivas habilidades dos voluntários. Esse uso não tem impacto significativo sobre as perspectivas de carreira futura e meios de subsistência dessas pessoas, mas combina conjuntos de habilidades e interesses relevantes com as atividades de voluntariado ou atribuições de curto prazo relevantes, liberando tempo para que os recursos sejam gastos em outras áreas.
IV – evaluation of criteria for access, eligibility, concession, revision, reduction or revocation of private and public services that are considered essential, including systems used to evaluate the eligibility of natural persons regarding the provision of public assistance and security services;	
V – assessment of the debt capacity of natural persons or establishment of their credit rating;	
VI – sending or establishing priorities for emergency response services, including firefighters and medical assistance;	
VII – administration of justice, including systems that assist judicial authorities in the investigation of facts and in the application of the law;	
VIII – autonomous vehicles, when their use may pose risks to the physical integrity of people;	
IX – applications in the health area, including those intended to aid diagnoses and medical procedures;	
X – biometric identification systems;	• Os "sistemas de identificação biométrica" devem ser claramente definidos no texto e o projeto de lei deve esclarecer se a intenção é diferenciá-los dos "sistemas de autenticação biométrica". Sistemas de identificação biométrica envolvem processamento de dados biométricos de um número indiscriminado de indivíduos e exigem comparação de dados biométricos de um indivíduo com dados biométricos de muitos outros indivíduos armazenados em um banco de dados para identificar esse indivíduo (ou seja, correspondência de um para muitos). Por outro lado, sistemas de autenticação biométrica podem acarretar menos riscos, já que consistem na comparação de dois modelos biométricos que normalmente se supõe pertencerem ao mesmo indivíduo (ou seja, correspondência de um para um). No entanto, o risco associado ao aplicativo biométrico depende, em última análise, da arquitetura da tecnologia, se os dados pessoais são coletados e armazenados e se isso ocorre por solicitação ou conhecimento de um indivíduo. Há implicações adicionais dependendo dos possíveis usuários de aplicativos biométricos (por exemplo, um agente estatal usando tecnologia de identificação para vigilância comparativamente a um usuário individual desbloqueando seu smartphone). Portanto, é importante que a Lei, ao considerar o risco associado aos sistemas de identificação biométrica, leve em conta o contexto do aplicativo biométrico.
XI – criminal investigation and public safety, in particular for individual risk assessments by the competent authorities, in order to determine the risk of a person committing offenses or of recidivism, or the risk to potential victims of criminal offenses or to assess personality traits and the characteristics or past criminal behavior of individuals or groups;	

XII – analytical study of crimes relating to natural persons, allowing police authorities to search large sets of complex data, related or unrelated, available from different data sources or in different data formats, in order to identify unknown patterns or discover hidden relationships in the data;	
XIII – investigation by administrative authorities to assess the credibility of evidence in the course of investigation or repression of infringements, to predict the occurrence or recurrence of an actual or potential infringement based on the definition of profiles of natural persons;	
XIV – migration management and border control.	
Art. 18. It will be up to the competent authority to update the list of excessive or high risk artificial intelligence systems, identifying new hypotheses, based on at least one of the following criteria:	• Fatores adicionais a serem levados em consideração: • Gravidade e probabilidade de danos a indivíduos, grupos ou à sociedade em geral (baseando-se em conclusões que podem ser alcançadas com razoável certeza); • Nível e significância de envolvimento humano, revisão e adequação de acordo com contexto; • Magnitude e probabilidade de benefício do uso de IA para indivíduos, grupos de indivíduos ou para a sociedade em geral; • Risco de reticência e/ou custos de oportunidade de não se usar a IA para indivíduos, grupos de indivíduos ou para a sociedade em geral. Isso incluiria a ponderação de benefícios do uso de IA em relação a deixar o processo no status quo atual (ou seja, medir se o resultado é aprimorado pelo uso de IA em vez de deixá-lo como está sendo feito atualmente); e • Medidas de mitigação para se lidar com os riscos. • A satisfação de um único critério não deve tornar automaticamente um sistema de risco alto ou excessivo. Em vez disso, a decisão deve refletir a consideração de todos os critérios relevantes listados no Artigo 18, bem como os possíveis benefícios do uso de risco potencialmente alto ou excessivo.
a) the implementation is on a large scale, taking into account the number of people affected and the geographic extent, as well as its duration and frequency;	
b) the system may negatively impact the exercise of rights and freedoms or the use of a service;	
c) the system has a high potential for material and moral damage, as well as being discriminatory;	
d) the system affects people from a specific vulnerable group;	• É importante a garantia de que os sistemas de IA não estejam causando discriminação ilegal ou tendo efeitos negativos específicos e perniciosos. A linguagem deve concentrar-se na prevenção de discriminação ilegal/abusiva e de seus efeitos danosos.
e) the possible harmful results of the artificial intelligence system are irreversible or difficult to reverse;	
f) a similar artificial intelligence system has previously caused material or moral damage;	• Serão necessários critérios para determinar se um sistema é semelhante a outro. Além disso, a disposição deve concentrar-se em contextos em que os sistemas serão usados e não nos sistemas em si.

g) low degree of transparency, explainability and auditability of the artificial intelligence system, which makes its control or supervision difficult;	
h) high level of identifiability of data subjects, including the processing of genetic and biometric data for the purpose of unique identification of a natural person, especially when the processing includes combining, matching or comparing data from several sources;	
i) when there are reasonable expectations of the affected person regarding the use of their personal data in the artificial intelligence system, in particular the expectation of confidentiality, as in the processing of confidential or sensitive data.	
Sole Paragraph. The updating of the list by the competent authority will be preceded by consultation with the competent sectoral regulatory body, if any, as well as public consultation and hearing and regulatory impact analysis.	• A atualização da lista de usos de alto risco é uma deliberação importante, que deve refletir os pontos de vista de todas as partes interessadas afetadas e considerar riscos e benefícios da tecnologia, além das compensações relacionadas.
GOVERNANCE OF ARTIFICIAL INTELLIGENCE SYSTEMS	
Art. 19. The artificial intelligence agents will establish governance structures and internal processes able to guarantee the security of the systems and the fulfillment of the rights of affected people, under the terms set forth in Chapter II of this Law and the relevant legislation, which will include, at least:	• Apoiamos firmemente os princípios do Artigo 19 - eles refletem conceitos fundamentais de uma abordagem baseada em responsabilização para a governança de sistemas de IA. Eles refletem conceitos refletidos na Estrutura de Responsabilização do CIPL, que tem sete elementos: Liderança e Supervisão, Avaliação de Risco, Políticas e Procedimentos, Transparência, Treinamento e Conscientização, Monitoramento e Verificação e Resposta e Aplicação. Para mais informações, consulte o Relatório de Mapeamento de Responsabilização do CIPL. • Pode-se incorporar elementos adicionais da Estrutura de Responsabilização aos requisitos do Artigo 19, como o estabelecimento de programas internos de treinamento e conscientização. • A estrutura regulatória também deve oferecer recompensas e incentivos adequados para estimular ainda mais e ajudar a acelerar a responsabilização de IA e as melhores práticas organizacionais. Esses "incentivos" podem incluir: vincular a comprovação de responsabilização a certificações externas; reconhecer compromissos autorregulatórios de organizações que definem publicamente valores e princípios de IA que elas implementam, juntamente com o progresso em relação a parâmetros de referência (benchmarks); usar a responsabilização demonstrada como uma "licença para operar", permitindo que organizações responsáveis e/ou certificadas tenham mais oportunidades de usar e compartilhar dados de forma responsável para facilitar o crescimento de usos responsáveis de IA; permitir o uso mais amplo de dados em IA para projetos socialmente benéficos; usar a responsabilização demonstrada de IA como critério para projetos de compras públicas ou due diligence (diligência devida) B2B; e reconhecer a responsabilização demonstrada de IA como fator mitigante ou redutor de responsabilidade no contexto da aplicação.

I – transparency measures regarding the use of artificial intelligence systems in the interaction with natural persons, which includes the use of adequate human-machine interfaces that are sufficiently clear and informative;	
II – transparency regarding the governance measures adopted in the development and use of the artificial intelligence system by the organization;	
III – appropriate data management measures to mitigate and prevent potential discriminatory biases;	
IV – legitimation of data processing in accordance with data protection legislation, including through the adoption of privacy measures by design and by default and the adoption of techniques that minimize the use of personal data;	
V – adoption of adequate data separation and organization parameters for training, testing and validation of system results;	
VI – adoption of appropriate information security measures from conception to operation of the system.	
Paragraph 1° The governance measures of artificial intelligence systems are applicable throughout their entire life cycle, from the initial conception to the closure of their activities and discontinuation.	• O ciclo de vida da IA é complexo e envolve uma variedade de atores ao longo do processo. A lei deve deixar claro que as obrigações podem diferir de acordo com a função que as entidades desempenham no ciclo de vida de IA.
Paragraph 2 The technical documentation of high-risk artificial intelligence systems will be prepared before they are made available on the market or used to provide a service and will be kept up to date during their use.	
Governance Measures for High-Risk Artificial Intelligence Systems	
Art. 20. In addition to the measures indicated in art. 19, artificial intelligence agents providing or operating high-risk systems will adopt the following governance measures and internal processes:	
I – documentation, in the appropriate format for the development process and the technology used, regarding the functioning of the system and the decisions involved in its construction, implementation and use, considering all relevant stages in the life cycle of the system, such as the stage of system design, development, evaluation, operation and retirement;	• A Lei deve adotar uma abordagem que ofereça flexibilidade no formato, desde que todos os elementos necessários sejam incluídos. • A Lei não deve, em nenhum caso, exigir documentação formal de cada decisão tomada no desenvolvimento de um sistema de IA. Frequentemente, vários atores interagem em diversas fases do desenvolvimento de um sistema de IA. Mesmo que cada interveniente documentasse as decisões tomadas nos seus respetivos ciclos de vida, é improvável que essas decisões representem adequadamente o nível de risco global do sistema, uma vez que este último dependerá de múltiplos fatores, incluindo o contexto de implantação.

II – use of tools for automatically recording the system's operation, in order to allow the assessment of its accuracy and robustness and to determine discriminatory potentials, as well as the implementation of adopted risk mitigation measures, with special attention to adverse effects;	
III – carrying out tests to assess appropriate levels of reliability, depending on the sector and the type of application of the artificial intelligence system, including robustness, accuracy, precision and coverage tests;	
IV – data management measures to mitigate and prevent discriminatory biases, including:	
a) evaluation of the data with appropriate measures to control human cognitive biases that may affect the collection and organization of the data, as well as measures to avoid the generation of biases due to classification problems, failures or lack of information regarding affected groups, lack of coverage or distortions in representativeness, depending on the intended application, as well as corrective measures to avoid the incorporation of structural social biases that can be perpetuated and amplified by technology;	• É importante abordar danos como o preconceito social, mas por vezes é difícil avaliá-los. Deverá ser solicitado às partes que demonstrem boa-fé e esforços razoáveis, baseando-se nas orientações disponíveis. As partes não devem ser penalizadas por decisões posteriormente consideradas incorretas e cujas avaliações foram realizadas de boa-fé.
b) composition of an inclusive team responsible for the design and development of the system, guided by the pursuit of diversity.	• Seria útil fornecer orientações sobre como a diversidade e a inclusão deveriam ser medidas para efeitos de cumprimento deste requisito.
V – adoption of technical measures to enable the explanation of the results of artificial intelligence systems and of measures to provide operators and potential impacted parties with general information on the functioning of the artificial intelligence model employed, explaining the logic and criteria relevant to the production of results, as well as, at the request of the interested party, provide adequate information that allows the interpretation of the concretely produced results, respecting industrial and commercial secrecy.	
Sole Paragraph. Human supervision of high-risk artificial intelligence systems will seek to prevent or minimize risks to the rights and freedoms of persons that may arise from their normal use or their use under reasonably foreseeable conditions of misuse, enabling the persons responsible for human supervision to:	
I – understand the capabilities and limitations of the artificial intelligence system and properly control its operation, so that signs of anomalies, dysfunctions and unexpected performance can be identified and resolved as quickly as possible;	
II – be aware of the possible tendency to automatically trust or rely excessively on the result produced by the artificial intelligence system;	

III – correctly interpret the result of the artificial intelligence system, taking into account the characteristics of the system and the tools and methods of interpretation available;	• O texto deve contar com linguagem que reconheça intervalos normais de probabilidade de ocorrência de erros, por exemplo, adicionar “margens normais de erro” após “características do sistema”.
IV – decide, in any specific situation, not to use the high-risk artificial intelligence system or to ignore, annul or reverse its result; and	
V – intervene in the operation of the high-risk artificial intelligence system or interrupt its operation.	
Art. 21. In addition to the governance measures established in this chapter, bodies and entities of the government of the Union, States, Federal District and Municipalities, when contracting, developing or using artificial intelligence systems considered to be of high risk, will adopt the following measures:	
I – holding a prior public consultation and hearing on the planned use of artificial intelligence systems, with information on the data to be used, the general operating logic and results of tests carried out.	
II – definition of protocols for accessing and using the system that allow the registration of who used it, for what concrete situation, and for what purpose;	
III – use of data from reliable sources, which are accurate, relevant, up-to-date and representative of the affected populations and tested against discriminatory biases, in accordance with Law No. 13,709, of August 14, 2018, and its regulatory acts;	• Os termos propostos nesta disposição requerem maior clareza e o projeto de lei, ou a orientação regulamentar subsequente, deverá fornecer indicações adicionais sobre como o setor público deverá implementar essas obrigações na prática.
IV – facilitated and effective guarantee to the citizen, before the government, of the right to human explanation and review of decision by artificial intelligence systems that generate relevant legal effects or that significantly impact the interests of the affected, to be carried out by the competent public agent;	
V – use of an application programming interface that allows its use by other systems for interoperability purposes, pursuant to regulations;	
VI – publication in easily accessible vehicles, preferably on their websites, of the preliminary assessments of the artificial intelligence systems developed, implemented or used by the public authorities of the Union, States, Federal District and Municipalities, regardless of the degree of risk, without prejudice to the provided in art. 43.	
Paragraph 1 The use of biometric systems by the government of the Union, States, Federal District and Municipalities will be preceded by the issuance of a normative act that establishes guarantees for the exercise of the rights of the affected person	• Será importante deixar claros os limites de aplicação dos direitos e obrigações desta Lei comparativamente àqueles a serem incluídos no ato normativo aqui mencionado. Se quaisquer obrigações desta Lei não se aplicarem a entidades do setor público, esta limitação na aplicação deverá ser explicitada.

and protection against direct, indirect, illegal or abusive discrimination, The processing of race, color or ethnicity data is prohibited, unless expressly provided for by law.	• É importante permitir o processamento de dados sobre raça, cor e etnia na medida necessária para identificar e prevenir a discriminação e o preconceito.
Paragraph 2 If it is impossible to eliminate or substantively mitigate the risks associated with the artificial intelligence system identified in the algorithmic impact assessment provided for in article 22 of this Law, its use will be discontinued.	• Considerar alterar o parágrafo 2 para estipular que as entidades governamentais devem avaliar e pesar os benefícios, bem como os riscos associados ao desenvolvimento e à implantação de sistemas de IA — e os riscos associados ao *não* desenvolvimento e implantação do sistema — no contexto das avaliações de impacto algorítmicas.
Algorithmic Impact Assessment	
Art. 22. The algorithmic impact assessment of artificial intelligence systems is an obligation of artificial intelligence agents whenever the system is considered as high risk by the preliminary assessment.	• A relação entre operadores e fornecedores deve ser esclarecida em termos de seus respectivos papéis e responsabilidades no que diz respeito à obrigação de avaliação de impacto. É provável que ambos precisem fazer avaliações de risco/impacto para avaliar os riscos que estão sob o seu controle durante a fase de desenvolvimento e a fase de implantação e utilização, respetivamente. • O projeto de lei e as autoridades podem esclarecer que a preparação de avaliações de impacto de boa-fé e em conformidade com os requisitos pode servir como um fator mitigante em um contexto de aplicação, o que serviria como incentivo adicional para fornecer avaliações de impacto completas e precisas.
Sole Paragraph. The competent authority will be notified of the high-risk system by sharing preliminary and algorithmic impact assessments.	• O projeto de lei deverá esclarecer se todas as partes que desenvolvem sistemas de alto risco são obrigadas a notificar a autoridade competente e se as partes precisam receber qualquer autorização explícita para prosseguir com o desenvolvimento ou a implantação. Exigir notificação de cada utilização de alto risco proposta poderia criar um processo que seria desnecessariamente oneroso, tanto para o governo como para as organizações que propõem sistemas de IA para desenvolvimento ou utilização. • O projeto de lei ou a orientação subsequente podem afirmar que a divulgação de uma avaliação de impacto algorítmica à autoridade competente não constitui uma renúncia a qualquer prerrogativa de sigilo (inclusive estabelecida por lei) ou proteção do produto de trabalho que possa existir em relação a qualquer informação contida nas avaliações de impacto algorítmicas.
Art. 23. The algorithmic impact assessment will be carried out by a professional or team of professionals with the technical, scientific and legal knowledge necessary to carry out the report and with functional independence.	• É apropriado exigir que, sempre que necessário, as avaliações de impacto algorítmicas sejam conduzidas de uma forma que estejam em conformidade com as melhores práticas padrão do setor. Esta disposição não deve determinar quais são essas normas ou como as entidades devem cumpri-las, uma vez que provavelmente variará substancialmente em todo o setor. Empresas maiores, por exemplo, podem criar processos internos, enquanto entidades menores podem utilizar serviços de terceiros.
Sole Paragraph. It will be up to the competent authority to regulate the cases in which the performance or audit of the impact assessment will necessarily be conducted by a professional or team of professionals external to the supplier;	• Auditorias externas de terceiros podem desempenhar um papel importante em qualquer estrutura de responsabilização, incluindo a responsabilização por IA. O projeto de lei deve estabelecer critérios claros para quando serão necessárias auditorias externas, tais como casos de risco extremamente elevado ou falta de vontade demonstrada para agir de forma responsável, como a constatação de incumprimento ou violação de uma ordem de execução anterior. • Idealmente, as auditorias externas são realizadas por entidades certificadas com o dever de proteger os interesses públicos e garantir o cumprimento dos critérios legais. Além disso, os investigadores públicos realizam frequentemente auditorias externas de terceiros para compreender melhor o impacto de produtos

	e serviços em determinados grupos. Mais uma vez, essas auditorias podem ajudar a aumentar a confiança, demonstrando que uma aplicação de IA possui as características necessárias. Além disso, as auditorias externas podem fornecer opiniões mais robustas e neutras sobre questões éticas e de conformidade particularmente difíceis e podem, portanto, ser vistas como mais críveis pelo público. Os requisitos de auditoria externa devem ser concebidos através de consulta às partes interessadas e atualizados regularmente com base nos desenvolvimentos tecnológicos e nas novas práticas.
	
	• Existem desafios específicos associados às auditorias externas de modelos e sistemas de IA, para conformidade com objetivos de IA confiáveis e não vinculativos, bem como com leis. Esses incluem:
	  ◦ Garantir que os implantadores forneçam transparência e aviso quando implantarem sistemas de IA;
	  ◦ Acessar os dados nos quais os modelos são treinados; e
	  ◦ Acesso a avaliações internas pré-implantação.
	• Além disso, antes de um modelo de IA ser testado quanto a tendências, ele deve ser testado quanto à funcionalidade. No entanto, os auditores e investigadores externos enfrentam frequentemente um problema de "caixa preta" e não conseguem recriar os modelos para testar a funcionalidade porque não têm acesso aos conjuntos de dados reais que foram utilizados para treinar o modelo.
	• Quer as avaliações sejam obrigatórias ou voluntárias, as organizações devem ter flexibilidade na forma como as conduzem, desde que cumpram determinados padrões e sejam produzidas mediante solicitação dos reguladores.
	
	• O fornecedor de um sistema de IA está em melhor posição para determinar como conduzir a avaliação de impacto e a mitigação de riscos para os sistemas de IA que desenvolveu. O regulador deve esforçar-se por fornecer um objetivo e/ou padrão para o fornecedor buscar, mas deve caber ao fornecedor escolher os melhores meios e processos para cumprir.

Art. 24. The impact assessment methodology will contain, at least, the following steps:	• Embora o projeto de lei (ou orientação regulamentar) deva fornecer modelos de avaliação de impacto detalhando os requisitos mínimos, deve manter uma abordagem flexível, desde que todas as considerações substantivas sejam incluídas com base no contexto do processamento. O projeto de lei também deve adotar uma abordagem que proporcione flexibilidade no formato em torno de certos elementos necessários.
I – preparation;	
II – risk cognition;	
III – mitigation of the risks found;	
IV – monitoring.	
Paragraph 1 The impact assessment will consider and record, at least:	

a) known and foreseeable risks associated with the artificial intelligence system at the time it was developed, as well as the risks that can reasonably be expected from it;	• Os riscos a registrar devem ser “razoavelmente” previsíveis.
b) benefits associated with the artificial intelligence system;	• A exigência de avaliar tanto os benefícios como os riscos é louvável. Isso permite um cálculo mais completo do impacto potencial.
c) likelihood of adverse consequences, including the number of people potentially impacted	• O conceito de “consequências adversas” deve ser esclarecido no projeto de lei ou através de orientações regulamentares adicionais, por uma questão de previsibilidade e rigor.
d) severity of adverse consequences, including the effort required to mitigate them;	• Ver item “c”, acima.
e) operating logic of the artificial intelligence system;	• Os autores do projeto de lei deveriam reconsiderar a exigência de incluir a lógica dos sistemas de IA nas avaliações de impacto. Sistemas lógicos semelhantes podem funcionar de forma diferente, dependendo da utilização do sistema, e as avaliações de impacto devem ser tecnologicamente neutras.
f) process and results of tests and evaluations and mitigation measures carried out to verify possible impacts on rights, with special emphasis on potential discriminatory impacts;	
g) training and actions to raise awareness of the risks associated with the artificial intelligence system;	
h) mitigation measures and indication and justification of the residual risk of the artificial intelligence system, accompanied by frequent quality control tests;	
i) measures of transparency to the public, especially to potential users of the system, regarding residual risks, especially when they involve a high degree of harmfulness or danger to the health or safety of users, pursuant to articles 9 and 10 of Law No. 8,078, of September 11, 1990 (Consumer Protection Code);	
Paragraph 2 In keeping with the precautionary principle, when using artificial intelligence systems that may generate irreversible impacts or those that are difficult to reverse, the algorithmic impact assessment will also take into account incipient, incomplete or speculative evidence.	• Qualquer evidência incipiente, incompleta ou especulativa utilizada deve ser descrita adequadamente. Embora essas evidências possam ser úteis, também podem ter limitações e é importante contextualizá-las.
Paragraph 3 The competent authority may establish other criteria and elements for the preparation of the impact assessment, including the participation of the different social segments affected, according to the risk and economic size of the organization.	• Dado que a avaliação de impacto será necessariamente feita para um grande número de sistemas de IA e por entidades grandes e pequenas, os critérios devem ser estabelecidos antecipadamente com clareza e rigor.
Paragraph 4 It will be up to the competent authority to regulate the periodicity of updating impact assessments, considering the life cycle of high-risk artificial intelligence systems and the fields of application, and may incorporate best sectoral practices.	• O projeto de lei (ou orientação regulamentar subsequente) deve especificar a periodicidade das avaliações de impacto. Uma abordagem razoável poderia ser que uma empresa apresentasse uma avaliação de impacto, de preferência em forma resumida, para atividades de processamento que atendam a um determinado limite de nível de risco no caso de quaisquer alterações materiais no processamento, o que poderia incluir alterações nos modelos de negócios, risco, legislação, tecnologia e outros fatores externos e internos.

Paragraph 5 The artificial intelligence agents who, after its introduction on the market or use in service, become aware of an unexpected risk that they present to the rights of natural persons, shall immediately communicate the fact to the competent authorities and to the people affected by the artificial intelligence system.	
Art. 25. The algorithmic impact assessment will consist of a continuous iterative process, performed throughout the entire lifecycle of high-risk artificial intelligence systems, requiring periodic updates.	• Ver comentários no Artigo 24 (parágrafo 4)
Paragraph 1 It will be up to the competent authority to regulate the periodicity of updating impact assessments.	
Paragraph 2 The update of the algorithmic impact assessment will also have public participation, based on a stakeholder consultation procedure, even in a simplified manner.	• Conforme descrito no Art. 23, as avaliações de impacto algorítmicas devem ser conduzidas por especialistas que operam de forma consistente com os padrões e melhores práticas do setor.
Art. 26. Industrial and commercial secrets being guaranteed, the conclusions of the impact assessment will be public, containing at least the following information:	• Ver comentários no Artigo 22 (parágrafo único)
I – description of the intended purpose for which the system will be used, as well as its context of use and territorial and temporal scope;	
II – risk mitigation measures, as well as their residual level, once such measures have been implemented;	
III – description of the participation of different affected segments, if it occurred, under the terms of Paragraph 3 of art. 24 of this Law.	
Civil Liability	• Comentário aplicável aos artigos 27-29: A adoção de mecanismos de responsabilização organizacional (*accountability*) por todos os atores do ecossistema de IA conduzirá a uma melhor conformidade e resultados práticos e provavelmente resultará em uma menor necessidade de se recorrer a questões relacionadas com a responsabilidade. • Quando surgem questões sobre responsabilidade civil, a atribuição entre os agentes de IA pode ser um desafio. Se uma determinada implantação de um sistema de IA, por exemplo, resultar em danos a um indivíduo, a responsabilidade deverá ser atribuída ao criador do sistema, ao implementador ou a alguma combinação, dependendo das circunstâncias do caso? Naturalmente, espera-se que o implementador realize uma avaliação de impacto do serviço, mas essa avaliação muitas vezes depende das informações que o desenvolvedor forneceu ao implementador para poder avaliar o modelo que está sendo incorporado ao serviço a ser implantado. Sem informações precisas, muitas vezes é difícil avaliar toda a gama de impactos no nível do implementador. Além disso, vale a pena notar que existem muitas salvaguardas que podem ser implementadas à montante para se evitar danos à jusante. • O projeto de lei poderia salientar que os reguladores devem procurar atribuir a responsabilidade de acordo

	com a quota-parte de responsabilidade das partes na geração do dano em questão, permanecendo conscientes de que as práticas contratuais também vão desempenhar um papel importante na definição e atribuição de responsabilidades e obrigações.
Art. 27. The supplier or operator of an artificial intelligence system that causes property, moral, individual or collective damage is obliged to fully repair it, regardless of the degree of autonomy of the system.	• A lei deve incentivar os operadores de sistemas de IA a envolverem-se em esforços adequados de avaliação e mitigação de riscos. Nos casos em que os operadores tenham agido razoavelmente e trabalhado para mitigar os riscos previsíveis, só deverão ser responsáveis pelos danos causados por sua própria negligência. Os operadores de sistemas de IA só devem ser responsabilizados pelos mais elevados níveis de responsabilidade quando violarem a lei e os seus sistemas causarem danos. • Os legisladores brasileiros podem, por exemplo, levar em consideração as medidas propostas na UE. Embora a responsabilidade não esteja explicitamente coberta pela Lei da UE sobre IA, uma proposta de Diretiva de Responsabilidade pela IA visa esclarecer o papel da responsabilidade civil por danos causados por sistemas de IA na ausência de relação contratual. Por conseguinte, o artigo 4.º da Diretiva introduziria uma presunção refutável de nexo de causalidade entre a culpa do requerido e os danos causados pelos sistemas de IA. Essa presunção seria aplicável, sujeita às três condições seguintes: • (i) o requerente demonstrou que o requerido não cumpriu um dever de cuidado destinado a proteger contra o dano ocorrido; • (ii) pode ser considerado razoavelmente provável, com base nas circunstâncias do caso, que a falha tenha influenciado o resultado produzido pelo sistema de IA ou a falha do sistema de IA em produzir um resultado; e • (iii) o requerente demonstrou que o resultado produzido pelo sistema de IA ou a falha do sistema de IA em produzir um resultado deu origem ao dano.
Paragraph 1 In the case of a high risk or excessive risk artificial intelligence system, the supplier or operator is objectively responsible for the damage caused, to the extent of their participation in the damage.	• Ver o comentário sobre Responsabilidade Civil acima. Além disso, o projeto de lei deve reconhecer as medidas proativas tomadas pelas organizações de boa-fé como um fator atenuante em um contexto de aplicação – isto servirá como um incentivo adicional para as organizações realizarem avaliações de risco. • A proposta de Diretiva de Responsabilidade da IA na UE, por exemplo, estabelece uma presunção de causalidade entre a culpa do requerido e o resultado produzido pelo sistema de IA ou a falha do sistema de IA em produzir um resultado. No entanto, no caso de um pedido de indenização relativo a um sistema de IA de alto risco, a presunção de causalidade não é aplicável quando o requerido demonstra que provas e conhecimentos especializados suficientes estão razoavelmente acessíveis para que o requerente possa provar o nexo de causalidade entre o alegado prejuízo e as ações do requerido (artigo 4º, nº 4). Essa possibilidade pretende incentivar os requeridos a cumprirem as suas obrigações de divulgação, com medidas estabelecidas pela Lei de IA para garantir um elevado nível de transparência de IA ou com requisitos de documentação e registro.
Paragraph 2 When it is not a high-risk artificial intelligence system, the guilt of the agent causing the damage will be presumed, applying the reversal of the burden of proof in favor of the victim.	• A linguagem aqui é confusa e não deixa claro se o ônus de provar os danos recai sobre a vítima ou sobre o agente. • Dependendo da forma como for interpretada, esta disposição poderá aumentar significativamente os custos associados ao desenvolvimento e à implantação de sistemas de IA de baixo risco, que estão rapidamente se tornando generalizados e indistinguíveis de outros sistemas computacionais lógicos.
Art. 28. Artificial intelligence agents will not be liable when:	

I – proving that they have not put into circulation, used or taken advantage of the artificial intelligence system; or	
II – proving that the damage is due exclusively to the victim or a third party, as well as an external fortuitous event.	
Art. 29. The hypotheses of civil liability arising from damage caused by artificial intelligence systems within the scope of consumer relations remain subject to the rules provided for in Law No. 8078, of September 11, 1990 (Consumer Protection Code), without prejudice to the application of other provisions of this Law	
Art. 30. Artificial intelligence agents may, individually or through associations, formulate codes of good practices and governance that establish the conditions of organization, operating regime, procedures, including complaints from affected people, safety standards , technical standards, specific obligations for each context of implementation, educational actions, internal mechanisms for supervision and risk mitigation, and appropriate technical and organizational security measures for managing the risks arising from the application of the systems.	• Enaltecemos as disposições do Artigo 30 que permitem aos agentes de IA formular códigos de boas práticas e governança e a disposição que estabelece que a participação em tais mecanismos será vista favoravelmente nas ações de aplicação da lei. • Seria útil orientação adicional que esclarecesse como a adesão aos códigos será monitorada e aplicada.
Paragraph 1 When establishing rules of good practices, the purpose and probability and gravity of the risks and resulting benefits will be considered, following the example of the methodology set forth in art. 24 of this law;	
Paragraph 2 The developers and operators of artificial intelligence systems may:	• Esta pode ser uma questão de tradução, mas esta é a primeira vez que o projeto de lei faz referência ao conceito de “desenvolvedor” – isto requer uma definição clara, especialmente no contexto da atribuição das responsabilidades e funções dos intervenientes no ciclo de vida da IA.
I – implement a governance program that, at a minimum:	
a) demonstrates its commitment to adopting internal processes and policies that ensure comprehensive compliance with rules and good practices regarding non-maleficence and proportionality between the methods employed and the determined and legitimate purposes of artificial intelligence systems;	
b) is adapted to the structure, scale and volume of its operations, as well as its harmful potential;	
c) has the objective of establishing a relationship of trust with the affected people, through transparent action and that ensures participation mechanisms under the terms of art. 24, Paragraph 3, of this Law;	
d) is integrated into its overall governance structure and establishes and applies internal and external oversight mechanisms;	
e) have response plans to reverse the possible harmful results of the artificial intelligence system;	
f) is constantly updated based on information obtained from continuous monitoring and periodic evaluations;	

Paragraph 3 Voluntary adherence to the code of good practices and governance can be considered an indication of good faith on the part of the agent and will be taken into account by the competent authority for the purpose of applying administrative sanctions.	• A lei deve incentivar os operadores de sistemas de IA a envolverem-se em esforços adequados de avaliação e mitigação de riscos e a participarem na adoção de boas práticas. Os operadores deverão ser incentivados a adotar tais práticas, por exemplo, atribuindo-lhes uma presunção de não negligência quando cumprem integralmente as boas práticas.
Paragraph 4 The competent authority may establish a procedure for analyzing the compatibility of the code of conduct with current legislation, with a view to its approval, publication and periodic updating.	
CHAPTER VII REPORTING SERIOUS INCIDENTS	
Art. 31. Artificial intelligence agents will report to the competent authority the occurrence of serious security incidents, including when there is a risk to the life and physical integrity of people, the interruption of operation of critical infrastructure operations, serious damage to property or the environment, as well as serious violations of fundamental rights, under the terms of the regulation.	
Paragraph 1 The reporting will be made within a reasonable time, as defined by the competent authority.	
Paragraph 2 The competent authority will verify the seriousness of the incident and may, if necessary, determine the agent to adopt measures to revert or mitigate the effects of the incident.	
CHAPTER VIII SUPERVISION	
Section I Competent Authority	
Art. 32. The Executive Branch shall designate the competent authority to ensure the implementation and supervision of this Law.	• Globalmente, muitas discussões vêm sendo realizadas sobre qual o órgão ou órgãos reguladores devem ser responsáveis pela IA. O Brasil deveria considerar que escopo pode existir para que a regulamentação seja executada pelos reguladores existentes. A ANPD terá um papel importante a desempenhar, já que muitas aplicações de IA envolvem o uso de dados pessoais. Para questões transversais fora do domínio da proteção de dados, tais como concorrência, propriedade intelectual e antidiscriminação (por exemplo, para habitação e emprego), outros reguladores podem ser importantes. Além disso, a utilização de IA é predominante em muitos setores, como cuidados de saúde e serviços financeiros, e os reguladores setoriais também terão interesse na regulamentação de IA no que diz respeito à utilização nos seus setores (consulte CIPL, AI and Data Protection in Tension (CIPL, IA e Proteção de Dados em Tensão, 2018) e o Livro Branco da CIPL sobre Ten Recommendations for Global AI Regulation (Dez Recomendações para Regulamentação Global de IA) para saber mais sobre a discussão a respeito de mudanças em setores-chave afetados por tecnologias emergentes de IA. • O Brasil deveria considerar a criação de um mecanismo para que os reguladores trabalhem juntos através de um centro regulatório ou outro fórum de cooperação (semelhante ao Fórum de Cooperação em Regulamentação Digital do Reino Unido) para garantir uma interpretação consistente das regras, supervisão e aplicação de IA. Pode-se também considerar estipular que este ou um órgão separado sirva como fonte de conhecimento especializado e aconselhamento ao governo e aos agentes de IA sobre tópicos técnicos, como padrões, ou sobre casos de uso específicos. O projeto de Lei da UE sobre IA contempla a criação de um órgão desta natureza (o “Conselho de Inteligência Artificial”).

	• Embora cada regulador deva manter competência sobre sua própria alçada (por exemplo, para fins de segurança jurídica, a ANPD deve manter competência geral sobre aplicações de IA que envolvam o processamento de dados pessoais e/ou que afetem a privacidade dos indivíduos), um órgão central permanente de coordenação governamental poderia definir políticas e metas de IA de alto nível aplicáveis em todos os setores e indústrias, além de facilitar o alinhamento, a coordenação regulatória e a ação conjunta entre diferentes órgãos reguladores, quando necessário e apropriado.
Sole Paragraph. It is up to the competent authority to:	• Não está claro se a autoridade competente é obrigada a realizar todas as atividades listadas neste parágrafo ou se alguma delas é discricionária. “Cabe à autoridade competente” deve ser interpretado neste contexto como sinônimo de “A autoridade competente irá”?
I – ensure the protection of fundamental rights and other rights affected by the use of artificial intelligence systems;	
II – promote the elaboration, updating and implementation of the Brazilian Artificial Intelligence Strategy with bodies with related authority;	
III – promote and prepare studies on good practices in the development and use of artificial intelligence systems;	
IV – encourage the adoption of good practices, including codes of conduct, in the development and use of artificial intelligence systems;	
V – promote cooperation actions with authorities for the protection and promotion of the development and use of artificial intelligence systems in other countries, of an international or transnational nature;	
a) procedures associated with the exercise of the rights provided for in this Law;	
b) procedures and requirements for preparing the algorithmic impact assessment;	
c) form and requirements of information to be published on the use of artificial intelligence systems; and	
d) procedures for certifying the development and use of high-risk systems.	
VII – articulate with public regulatory authorities to exercise their competences in specific sectors of economic and governmental activities subject to regulation;	
VIII – inspect, independently or jointly with other competent public bodies, the disclosure of information provided for in arts. 7 and 43;	
IX – inspect and apply sanctions in the event of development or use of artificial intelligence systems carried out in violation with legislation, through an administrative process that ensures contradictory, ample defense and the right of appeal;	
X – request, at any time, public authorities that develop or use artificial intelligence systems, a specific report on the scope, nature of the data and other details of the processing carried out, with	

the possibility of issuing a complementary technical opinion to guarantee compliance with this Law;	
XI – enter into, at any time, a commitment with artificial intelligence agents to eliminate irregularities, legal uncertainty or contentious situations within the scope of administrative proceedings, in accordance with the provisions of Decree-Law No. 4,657, of September 4, 1942;	
XII – consider petitions against the operator of the artificial intelligence system after proven submission of a complaint that has not been resolved within the period established by regulation; and	
XIII – prepare annual reports about its activities.	
Sole Paragraph. When exercising the authorities of the main sentence, the competent body may establish conditions, requirements, communication channels and differentiated disclosure for suppliers and operators of artificial intelligence systems qualified as micro or small companies, under the terms of Complementary Law No. 123, of December 14 2006, and startups, pursuant to Complementary Law No. 182, of June 1, 2021.	
Art 33. The competent authority will be the central body for the application of this Law and the establishment of norms and guidelines for its implementation.	
Art 34. The competent authority and the bodies and public entities responsible for regulating specific sectors of economic and governmental activity will coordinate their activities, in the corresponding spheres of action, with a view to ensuring compliance with this Law.	
Paragraph 1 The competent authority shall maintain a permanent forum for communication, including through technical cooperation, with public administration bodies and entities responsible for regulating specific sectors of economic and governmental activity, in order to facilitate their regulatory, inspection and sanctioning authorities.	
Paragraph 2 In experimental regulatory environments (regulatory sandbox) involving artificial intelligence systems, conducted by public bodies and entities responsible for regulating specific sectors of economic activity, the competent authority will be informed, being able to express its opinion regarding the fulfillment of the purposes and principles of this law.	• Prever a criação de ambientes de experimentação regulatória é um aspecto positivo da lei. A implementação desta disposição deve ser consistente com a iniciativa de sandbox regulatório anunciada pela ANPD em outubro de 2023.
Art 35. The regulations and rules issued by the competent authority shall be preceded by public consultation and hearing, as well as regulatory impact analysis, pursuant to arts. 6 to 12 of Law No. 13,848, of June 25, 2019, where applicable.	
Section II Administrative Sanctions	
Art. 36. AI agents, due to violations committed to the rules set forth in this Law, are subject to the following administrative sanctions applicable by the competent authority:	
I – warning;	
II – simple fine, limited, in total, to BRL 50,000,000.00 (fifty million Brazilian Real) per infraction, being, in the case of a legal entity governed by private law, up to 2% (two percent) of its revenue , of its group or conglomerate in Brazil in its last fiscal year, excluding taxes;	
III – publication of the infraction after its occurrence has been duly investigated and confirmed;	
V – prohibition or restriction to participate in the regulatory sandbox regime provided for in this law, for up to five years; and	

IV – partial or total suspension, temporary or definitive, of the development, supply or operation of the artificial intelligence system;	
VI – Prohibition of processing certain databases.	
Paragraph 1 The sanctions will be applied after an administrative procedure that allows the opportunity for full defense, gradually, separately or cumulatively, according to the peculiarities of the specific case and considering the following parameters and criteria:	
I – the seriousness and nature of the infractions and the eventual violation of rights;	
II – the good faith of the offender;	
III – the advantage earned or intended by the offender;	
IV – the economic condition of the offender;	
V – recurrence;	
VI – the degree of damage;	
VII – the cooperation of the offender;	
VIII – the repeated and demonstrated adoption of internal mechanisms and procedures capable of minimizing risks, including algorithmic impact analysis and effective implementation of the code of ethics;	• Elogiamos a inclusão deste fator de mitigação, que apoia uma abordagem à governança de IA baseada em responsabilização organizacional.
IX – the adoption of a policy of good practices and governance;	• Sugerimos acrescentar que a aquisição de certificações externas relevantes também deve ser tratada como um meio de demonstrar compromisso com a responsabilização organizacional e como um fator atenuante.
X – prompt adoption of corrective measures;	
the proportionality between the seriousness of the fault and the intensity of the sanction;	
XII – cumulation with other administrative sanctions that may have already been definitively applied for the same unlawful act.	
Paragraph 2 Before or during the administrative process of Paragraph 1, the competent authority may adopt preventive measures, including a fine, subject to the total limit referred to in item II of the main sentence, when there is evidence or well-founded fear that the intelligence agent artificial:	
I - causes or may cause damage that is irreparable or difficult to repair, or	
II – makes the final result of the process ineffective.	
Paragraph 3 The provisions of this article do not replace the application of administrative, civil or criminal sanctions defined in Law No. 8078, of September 11, 1990, Law No. 13709, of August 14, 2018, and in specific legislation.	
Paragraph 4 In the case of the development, supply or use of artificial intelligence systems of excessive risk, there will be, at least, the imposition of a fine and, in the case of a legal entity, the partial or total, provisional or definitive suspension of its activities.	
Paragraph 5 The application of the sanctions provided for in this article does not exclude, under any	

circumstances, the obligation to fully repair the damage caused, under the terms of art. 27.	
Art. 37. The competent authority will define, by means of its own regulation, the investigation procedure and criteria for the application of administrative sanctions for violations of this Law, which will be subject to public consultation, without prejudice to the provisions of Decree-Law No. 4,657, of 4 of September 1942, Law No. 9784 of January 29, 1999, and other relevant legal provisions.	
Sole Paragraph. The methodologies referred to in the main sentence of this article will be published in advance and will objectively present the forms and dosimetries of the sanctions, which will contain detailed reasoning for all its elements, demonstrating compliance with the criteria provided for in this Law.	
Section III Measures to foster innovation	
Art 38. The competent authority may authorize the functioning of an experimental regulatory environment for innovation in artificial intelligence (regulatory sandbox) for entities that request it and fulfill the requirements specified by this law and in regulations.	
Art. 39. Authorization requests for regulatory sandboxes will be submitted to the competent body through a project whose characteristics include, among others:	
a) innovation in the use of technology or in the alternative use of existing technologies;	
b) improvements in terms of efficiency gains, cost reduction, increased safety, risk reduction, benefits to society and consumers, among others;	
c) discontinuity plan, with predictions of measures to be taken to ensure the operational viability of the project once the regulatory sandbox authorization period has ended.	
Art. 40. The competent authority will issue regulations to establish the procedures for requesting and authorizing the operation of regulatory sandboxes, being able to limit or interrupt their operation, as well as issue recommendations, taking into account, among other aspects, the preservation of fundamental rights, of rights of potentially affected consumers and the security and protection of personal data that are subject to processing.	
Art. 41. Participants in the artificial intelligence regulatory testing environment continue to be liable, under the terms of the applicable liability legislation, for any damages inflicted on third parties as a result of the experimentation that takes place in the testing environment.	• A participação em um sandbox demonstra o compromisso de trabalhar em colaboração com os reguladores na implementação responsável de tecnologias emergentes. Em reconhecimento deste compromisso e para incentivar o uso do sandbox regulatório, recomendamos que a participação no sandbox seja tratada como um fator mitigante significativo nas ações de fiscalização se a alegada violação estiver relacionada a uma atividade que fez ou faz parte da sandbox.
Art. 42. The automated use of works, such as extraction, reproduction, storage and transformation, in data and text mining processes in artificial intelligence systems, in activities carried out by organizations and institutions of research, journalism and by museums, archives and libraries does not violate copyrights, provided that:	
I – it does not have the objective of simply reproducing, displaying or disseminating the original work itself;	
II – the use takes place to the extent necessary for the purpose to be achieved;	

III – it does not unjustifiably harm the data subjects' economic interests; and	
IV – it does not compete with the normal exploitation of the works.	
Paragraph 1 Any reproductions of works for the data mining activity will be kept under strict security conditions, and only for the time necessary to carry out the activity or for the specific purpose of verifying the results of the scientific research.	
Paragraph 2 The provisions of the main sentence apply to data and text mining activities for other analytical activities in artificial intelligence systems, subject to the conditions set out in the main sentence and paragraph 1, provided that the activities do not communicate the work to the public and that access to the works was given legitimately.	
Paragraph 3 The text and data mining activity involving personal data will be subject to the provisions of Law No. 13,709, of August 14, 2018 (General Law for the Protection of Personal Data).	
Section III Artificial intelligence public database	
Art. 43. It is up to the competent authority to create and maintain a high-risk artificial intelligence database, accessible to the public, which contains the public documents of the impact assessments, respecting commercial and industrial secrets, under the terms of the regulation.	• Temos preocupações sobre a viabilidade e conveniência de tal base de dados, conforme observado em nosso comentário ao Artigo 22, Parágrafo Único, acima. Se o governo estabelecer a base de dados, o acesso deverá estar sujeito a salvaguardas adequadas para garantir a confidencialidade de dados pessoais e de informações comerciais proprietárias.
CHAPTER IX FINAL PROVISIONS	
Art. 44. The rights and principles expressed in this Law do not exclude others provided for in the national legal framework or in international treaties to which the Federative Republic of Brazil is a party.	
Art. 45. This law comes into force one year after its publication.	