CIPL Comments on Brazilian Senate Bill No. 2338

Executive Summary and Relevant Context for CIPL Comments

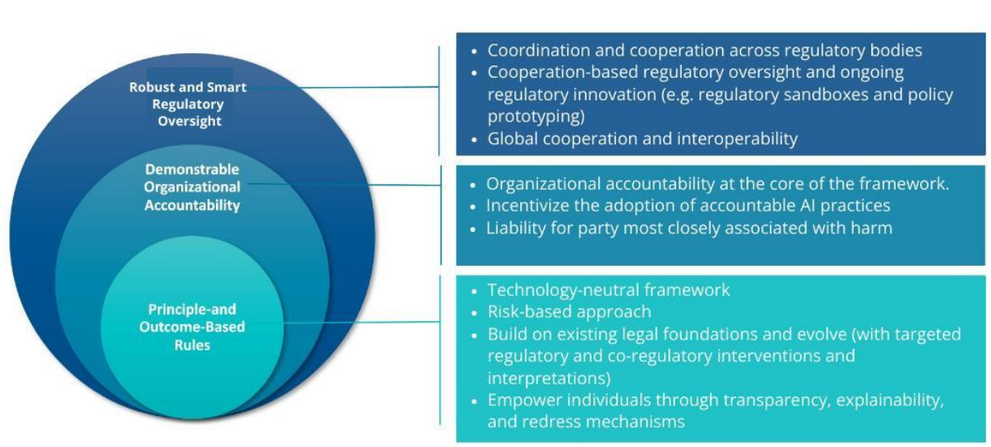
The Centre for Information Policy Leadership (CIPL)[1] commends the authors of Bill 2338 for crafting legislation on artificial intelligence (AI) centered on a risk-based approach and grounded in organizational accountability. CIPL has been a thought leader on organizational accountability and a risk-based approach to data policy and practices for over 20 years, and was an early contributor toward scoping challenges and defining solutions for AI governance and industry practices.[2] CIPL has also prepared detailed responses to public consultations on AI policy in Brazil, the European Union, the United Kingdom, and the United States.[3]

Drawing on this experience and our extensive engagement with private sector leaders developing and deploying AI technologies, policymakers, and regulators, in our recent publication *Ten Recommendations for Global AI Regulation*, CIPL offers recommendations to guide AI policymaking and regulation to enable accountable, responsible, and trustworthy AI. CIPL recommends a risk-based and tiered approach to regulating AI that builds on existing laws and standards and on accountable practices of organizations. This approach should be backed by innovative regulatory oversight and co-regulatory instruments. Any legislative or regulatory approach to AI should follow these overarching recommendations, which also encapsulate CIPL's view on a layered or three-tiered approach to AI regulation:

A. Principle-and Outcome-Based Rules
   1. Create a flexible and adaptable framework that defines the outcomes to be achieved, rather than prescribing details of how to achieve them
   2. Adopt a risk-based approach that considers risks and benefits holistically
   3. Build on existing hard and soft law foundations
   4. Empower individuals through transparency, explainability, and mechanisms for redress

B. Demonstrable Organizational Accountability
   5. Make demonstrable organizational accountability a central element of AI regulations
   6. Advance adoption of accountable AI governance practices
   7. Apportion liability carefully, with a focus on the party most closely associated with generating harm

C. Smart Regulatory Oversight
   8. Create mechanisms for coordination and cooperation across regulatory bodies
   9. Institute cooperation-based regulatory oversight and enable ongoing regulatory innovation
   10. Strive for global interoperability



[1] CIPL is a global privacy and data policy think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 85+ member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators, and policymakers around the world. For more information, please see CIPL's website at http://www.informa-tionpolicycentre.com/. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

[2] Key CIPL contributions in this space include *Artificial Intelligence and Data Protection in Tension* (October 2018), *Hard Issues and Practical Solutions* (February 2020), *Artificial Intelligence and Data Protection: How the GDPR Regulates AI* (March 2020), and *Ten Recommendations for Global AI Regulation (October 2023)*.

[3] CIPL Response to NTIA Request for Comment on AI Accountability Policy (June 2023); CIPL's Top Ten Recommendations for Regulating AI in Brazil (October 2022); CIPL Response to UK DCMS Proposed Approach to Regulating AI (September 2022); CIPL Response to the EU Commission's Consultation on the Draft AI Act (July 2021).

It is encouraging to see these recommendations adopted across many aspects of the Brazil draft legislation. At the same time, we have identified ways that the bill could be amended to further advance organizational accountability for responsible governance of AI, as well as areas where additional guidance or clarifications would be helpful. The following constitutes a summary of CIPL's key observations and recommendations:

- **Clarification on terminology –** the draft Bill uses some concepts and terms that require further specification for clarity. Notable examples include the definition of artificial intelligence; the concepts of AI supplier, operator, and agent; people affected by AI systems; the right to prior information regarding interactions with AI systems; and emotion recognition systems and biometric categorization systems. CIPL encourages the draft Brazil AI Bill to leverage existing and emerging soft law frameworks and their terminologies, such as those produced by the Organisation for Economic Co-operation and Development (OECD), which can foster international alignment on AI regulations.

- **Risk-based approach that considers risks and benefits holistically –** CIPL supports the draft Brazil AI Bill's risk-based approach that assigns obligations and governance models depending on the risk associated with AI systems. In doing so, rather than regulating the technology itself, the Bill regulates the risks that can result in undesired harms. CIPL also endorses the draft Bill's holistic risk-based approach that requires algorithmic impact assessments to include both the risks and benefits of a particular AI system.

- **Need for rebuttable presumption –** While the draft Bill prescribes a blanket prohibition of AI systems producing excessive risk and enumerates high-risk AI systems, CIPL recommends the Bill treat the level of risk as a rebuttable presumption. This would enable organizations to consider the highly contextual nature of AI applications and give them the opportunity to demonstrate that the use of an AI application in a specific context does not present an excessive or high risk.

- **Relationship with existing frameworks –** The draft Bill should avoid duplicating or creating any conflicting requirements with existing frameworks, such as the LGPD, consumer protection, anti-discrimination, and IP laws. While the language appears to make clear that the AI regulation is applicable without prejudice to the LGPD, it would be helpful to clarify which statute's requirements prevail in the event of any ambiguities or perceived conflicts.

- **Empowering individuals through responsible AI principles –** CIPL supports the draft Bill's approach to empowering individuals through transparency, explainability and mechanisms for redress, which will be instrumental in achieving trustworthy and beneficial AI. Nevertheless, the draft Bill or further regulatory guidance should clarify that developers and deployers of AI should provide context-appropriate and meaningful transparency and explainability about the inputs and operations of AI systems, while preserving other policy objectives, such as privacy, trade secrets, and security.

- **Demonstrable organizational accountability –** CIPL applauds the draft Bill for enabling AI agents to formulate codes of good practice and governance, and for stating that participation in such mechanisms will be viewed favorably in enforcement actions.

- **Modern approach to regulatory oversight –** CIPL endorses the draft Bill's approach to creating a regulatory sandbox for the purpose of encouraging innovation in AI. This will provide supervised safe spaces for organizations to address and resolve some of the more challenging aspects of deploying AI applications, particularly when they appear inconsistent or in tension with prevailing legal requirements. Nevertheless, CIPL is concerned about the continuous liability of participants in the testing environment and recommends that participation in the sandbox be treated as a significant mitigating factor in enforcement actions if the alleged violation relates to an activity that was or is part of the sandbox.

- **Liability allocation –** The AI lifecycle is complex and involves numerous actors with varied responsibilities throughout the process. The draft Bill should not treat all actors within the process similarly, as it would create significant negative effects on smaller entities, open-source developers, and innovators. The draft Bill and further regulatory guidance should target appropriate liability apportionment across parties in the AI ecosystem according to their share of responsibility for generating the harm in question and ability to mitigate such harm. CIPL also encourages the Bill to recognize proactive measures taken by organizations in good faith as a mitigating factor in an enforcement context. This will serve as an additional incentive for organizations to carry out risk assessments.

- **Coordination and cooperation across regulatory bodies –** CIPL supports the draft Bill's approach to promoting cooperative actions with domestic and international authorities for the protection and promotion of the development and use of AI systems. This approach would benefit both organizations and regulators by fostering consistency in regulatory approaches, as well as holistic and inter-disciplinary policy and guidance that is easier to implement and monitor by specialized regulators and industry over time.

- **Confidentiality of algorithmic impact assessments –** CIPL has concerns about the feasibility and advisability of a high-risk AI database prescribed in the draft Bill. Access to such a database should be subject to appropriate safeguards to ensure the confidentiality of personal data, proprietary business information, and other information that could be leveraged by malicious actors to circumvent the intended purpose of AI (e.g., a fraud prevention solution) or otherwise cause harm. The bill might also affirm that the disclosure of an algorithmic impact assessment to the competent authority does not constitute a waiver of any attorney-client privilege or work-product protection that might exist with respect to any information contained in the algorithmic impact assessments.

Finally, CIPL would like to draw attention to certain initiatives in the global arena toward development of international principles and standards, reflecting shared understandings and values arrived at through multistakeholder development processes. For instance, the G7 Digital and Tech Ministers reaffirmed the key role of standards at their Hiroshima Summit in April 2023, and G7 Leaders announced the Hiroshima Process International Guiding Principles for Organizations Developing Advanced AI Systems and the Hiroshima Process International Code of Conduct for Organizations Developing Advanced AI Systems in October. G7 Ministers are also working to develop a Comprehensive Policy Framework, to include cooperation with the Global Partnership on AI (GPAI) and Organisation for Economic Co-operation and Development (OECD). CIPL believes that the Brazil AI regulation should consider the aforementioned frameworks to achieve international alignment.

We would welcome the opportunity to answer any questions about our feedback and assist further with this important legislative effort.

ENG Version	COMMENTS
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:	• It will be important to clarify the extent to which Articles 2 and 3 are intended to be enforceable, and if so, how they will be enforced. • We recommend that the standard for these principles be the ability to demonstrate that actors have worked in good faith to give effect to these principles. This approach allows for mistakes – and correction of those mistakes – so long as they were not intentional or due to recklessness or negligence. • In addition, we suggest that the Bill add the following as a basis for the "development, implementation, and use of AI systems in Brazil": "XI – The need to consider and achieve, where possible and appropriate, global interoperability, convergence or harmonization with regard to AI technologies and applicable policies and regulations."
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;	• It is important to understand how justice, equity and inclusion will be assessed in practice, and in relation to other provisions such as non-discrimination (IV) and self-determination and freedom of decision and choice (II).
VI – transparency, explainability, intelligibility and auditability;	
VII – reliability and robustness of artificial intelligence and information security systems;	• It will be important to understand how reliability and robustness will be assessed in practice. At the same time, any guidance on this should avoid creating prescriptive obligations that burden organizations unnecessarily.
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;	• It is important to create an environment that encourages innovation and investment, while also protecting consumers. That requires striking a balance that encourages responsible innovation. • There should be limits on AI developers' and providers' liability for damages if they have acted responsibly, or lack the ability to prevent or otherwise avoid harm stemming harm from other AI actors.

XI – prevention, precaution and mitigation of systemic risks derived from intentional or unintentional uses and unforeseen effects of artificial intelligence systems; and	• AI developers and providers should be encouraged to anticipate and mitigate the reasonably foreseeable effects (including reasonably foreseeable misuse) of their systems. But to hold them responsible for all effects, no matter how difficult to foresee, could discourage investment and innovation in AI systems.
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.	• It is important for the Bill to provide a definition of AI that is identical to, or interoperable with, emerging global standard definitions such as that developed by the Organisation for Economic Co-operation and Development (OECD): "*An AI system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment.*" • The current definition of AI in the draft Bill is overly broad, which risks applying to virtually all kinds of software, rather than targeting specific risks the Bill is purporting to address. In particular, the current formulation not only includes "machine learning approaches" of various kinds, but also includes all "logic and knowledge representation". This could virtually include any computerized software, even those that do not present the risks the Bill attempts to address. In order to ensure consistent application, the output (predictions, recommendations or decisions) generation element of the definition should be clarified in such a way that it covers system-generated AI outcomes, i.e., AI systems whose outputs are generated based on rules stemming from the AI system itself, not human-generated ones, such as a sophisticated excel sheet, the logic of which is fully developed and controlled by humans.

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;	• Comments on II, III, IV:
	
	• The typology of AI actors in the Bill bears some similarities but also key differences to regulatory frameworks in other jurisdictions. Brazil may wish to consider how these convergences and divergences could affect interoperability of Brazil's legislation with laws in other jurisdictions. Brazil may consider leveraging soft law frameworks such as the UNCITRAL AI actors taxonomy, that can foster international alignment on AI regulations. Accordingly, using the OECD recommendations as bases, UNCITRAL divides the actors involved in AI systems into four broad categories, namely:
	
	  ◦ "(a) *developer*: the person who is responsible for the AI system's theoretical high-level design, programming, training and verification, and interfacing and integration with external hardware, applications and data sources before deployment;
	
	  ◦ (b) *data provider*: the person who provides – or is responsible for providing – data to the system (i.e., the data needed to support training, deployment or operation);
	
	  ◦ (c) *deployer*: the person who deploys the system by integrating it into its operations (e.g., the goods and services that it supplies), including by setting up, managing, maintaining and supporting the supply of data and infrastructure necessary for the operation and monitoring of the AI system and its interaction with the supplied data once deployed;

	• (d) *operator*: the person who operates the system:
	  • (i) in many cases, the operator will be the person who deploys the system;
	  • (ii) in some cases, the operator may be the end user of AI-enabled goods or services (e.g., if the end user has some control over the operation of the goods or services);
	• (e) *affected person*: any other person affected by the operation of an AI system, including by interacting with the system (e.g., by providing data to the system) or being the end user of AI-enabled goods or services."
	• There are important questions that will need clarification with respect to the bounds of each definition, and where specific examples would fall. For example, if an entity procures a general-purpose AI system and then customizes features within it prior to deployment, will it be treated as a supplier?
	• Is "supplier" used interchangeably with "provider" in this bill?

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.	• See above (Article 4/II).
IV – artificial intelligence agents: providers and operators of artificial intelligence systems.	• See Comments on above (Article 4/II) – "agents" here seems close to the role of "operators" under the EU AI Act. Guidance may help clarify further.
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.	• Comment on VI and VII: Discrimination and indirect discrimination are important concepts – one will want to make sure that these concepts are consistent here with how they may be defined elsewhere in Brazilian law, e.g., the Statute for Racial Equality, to ensure consistent protections.
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:	• The concept of "people affected by AI systems" needs to be clarified, unless that has a specific meaning in other legislation or jurisprudence. The concept provides a list of rights; hence, it is important to provide clarification and legal certainty on text. Otherwise, it is likely to address everyone. Also, the Bill does not prescribe jurisdictional boundaries or ask individuals to have a specific nexus with Brazil. One may wish to clarify whether such nexus will be required for individuals to be covered by the law. • LGPD Article 20 specifies that an "affected person" with respect to automated decision making is someone who is (a) subject to a decision made solely via automated processing of personal data; (b) when that decision affects his/her personal, professional, consumer and credit profile, or aspects of her/his personality. If the concept of "affected" is intended here to be broader than the conditions specified in LGPD, additional guidance could help provide certainty.
I – right to prior information regarding their interactions with artificial intelligence systems;	• "Interaction" may need further specification for clarity. Is the intent to cover all circumstances in which individuals actively interact with an AI system, or would it also encompass circumstances in which an individual's data is processed by an AI system without active interaction from the individual? • Additional guidance or rules will be helpful to indicate clearly what sorts of information should be shared with individuals. There should be an effort to provide them information that is useful and not so excessive as to lead to "notice fatigue." Information must be provided with careful consideration of the consumers' ability to understand the information provided, to assess the consequences, and to make decisions based on it. These transparency obligations should be consistent with those mandated under LGPD. • Applying the principles of a risk-based approach is vital: information should be provided to address risks to the fundamental rights of individuals, in a form and to the extent it is useful and actionable.
II – right to an explanation about the decision, recommendation or predictions made by artificial intelligence systems;	• Explainability and transparency should be balanced with other policy objectives (e.g., IP rights, trademark, security of source code etc.). Dialogue is still ongoing within the AI community around how best to advance AI explainability and increase meaningful transparency. The Bill should also clarify the provision's relationship with Article 20(1) of the LGPD, prescribing that the controller shall provide, whenever requested, clear and adequate information regarding the criteria and procedures used for the automated decision, in compliance with commercial and industrial secrets. • The scope of disclosure needs to be clarified – see, for example, guidance prepared by the UK ICO on AI explainability. Overly broad disclosure may result in bad actors accessing information for inappropriate purposes, and may not be understood by individuals if provided in an overly technical format. Organizations should be required to find simple ways to inform individuals about the rationale behind or the criteria relied on in reaching the decision without providing a complex explanation of the algorithms used in circumstances where such disclosure is unlikely to be helpful – although there should be such be avenues for regulators and researchers to access such information in appropriate circumstances. • Providing appropriate transparency is contextual and rules on transparency should be flexible enough to accommodate different use cases. The Bill should not refer to just one approach to explaining decisions made with the help of AI, or to providing a single type of information to affected individuals. Instead, the context affects which type of explanation organizations use to make an AI-assisted decision clear or easy for individuals to understand. • The existing language means that affected individuals may invoke this right for any AI systems; however, in

	line with the risk-based approach, it should only be applicable to higher-risk use cases. • The concept of “decision" requires clarification as to which activities will be within scope.
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;	• While legal effects are relatively easy to identify, it is important for authorities to provide examples of automated decisions producing similarly significant effects.
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;	• The Bill’s approach to consider the state of the art and context is positive; however, the right to human participation should be structured within a risk-based approach that couples a right to request post-processing review—and redress in the event that a harm is identified—with robust *ex-ante* risk assessment and measures to mitigate the risk of potential harms.
V – right to non-discrimination and correction of direct, indirect, illegal or abusive discriminatory biases; and	• The Bill should include language emphasizing that it intends to limit illicit and harmful discrimination only.
VI – the right to privacy and protection of personal data, under the terms of the relevant legislation.	• This language appears to make clear that the AI regulation is applicable without prejudice to the LGPD. It would be helpful to clarify which statute’s requirements prevail in the event there are any ambiguities or perceived conflicts.
Sole paragraph. Artificial intelligence agents will inform, in a clear and easily accessible way, the procedures necessary for the exercise of these rights.	• The agent is defined as providers and operators of AI system. Additional legislative text, or follow-on guidance, would be useful to clarify the bounds of providers’ responsibilities vs. operators’.
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.	• As noted above, the Bill defines “people affected by AI systems” broadly (Article 5) and appears to give anyone, including those who don’t have specific connection or nexus with Brazil, the right to invoke the interests and rights provided in this Bill. It would be helpful to clarify if this is the intended scope of application.
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 intelligence system, clear and adequate information regarding the following aspects:	• As noted above, the concept of “people affected by AI systems” needs to be clarified, unless that has a specific meaning in Brazil’s legal framework. • It would be useful to clarify the roles and responsibilities of providers vs. operators (or other AI actors along the lifecycle) for providing this information, to avoid possible duplication or lack of compliance. • The Bill should acknowledge that the meaning of effective transparency in the AI context depends on the nature of the intended audience, which will inform the level and type of information to be provided.
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	• Transparency on security measures must be properly balanced against business trade secret imperatives, as well as security risks that could be a consequence of revealing to bad actors too much detail about how security mechanisms operate. • The meaning of "coverage" should be clarified.
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.	• "Emotion recognition systems" and "biometric categorization systems" should be clearly defined and should align with the LGPD's existing protections for sensitive personal data. It is important to note that there is an active debate internationally on which systems should and should not be within the scope of regulations for biometric systems; it will be important for the law to provide clarity on relevant provisions in this law.
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.	• The Bill should clarify the concept of "vulnerable group." Is it intended to be consistent with the LGPD (e.g., Art 14 LGPD – processing of children and adolescents' personal data)? • It may be useful to qualify the requirement with "to the extent possible" to enable provision of services in some circumstances where it may not be possible to enable such understanding (e.g., for very young or elderly and infirm individuals), and where fiduciaries may be able to act on their behalf.
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:	• The Bill should encourage organizations to develop best practices on AI explainability and transparency, as part of accountability and responsible and ethical development and use of technology. • The Bill should avoid prescribing access rights in a manner that would require organizations to provide overly detailed descriptions of complex algorithms behind automated decisionmaking processes. This is particularly important to ensure that businesses can provide meaningful information to average consumers about the underlying automated decisions and their logic. Full transparency of algorithms (i.e., disclosure of source code or extensive descriptions of the inner workings of algorithms) is not meaningful to users and

	does not advance their understanding of how their data is being handled in ADM processes. • Transparency and explainability rights must be balanced with businesses' legitimate interests in protecting their trade secrets and similar types of information, e.g., intellectual property rights, that would be put at risk through detailed disclosure requirements. • The pervasiveness of AI systems is such that imposing transparency and explainability obligations to all of them would not be impactful or even meaningful for the user. Rather, in line with the risk-based approach that should be underpinning AI legislation, these requirements should apply to the AI systems classified as having a higher risk of harm, not every single application.
I – the rationality and logic of the system, as well as the meaning and expected consequences of such a decision for the affected person;	• Organizations should have the flexibility to weigh this requirement against their legitimate interests like IP rights. Also, it may not always be technically possible to describe the logic of the system; hence, the Bill should include the flexibility language of "where possible and appropriate". • Rules on explainability must be formed in a way that privileges relevance for the affected person. The complexity of some AI systems, may make it infeasible to provide detailed information on every parameter and instruction used to guide decision making in a manner that is understandable and useful to an end user.
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;	• Requiring disclosure of full data sets risks overwhelming users with large amounts of information that may not be useful, while also creating privacy and trade secret risks. • It is important to provide information that is contextually valuable to affected people, while still preserving incentives for companies to build and maintain data sets and enabling them to protect against risks to privacy and other harms that could result from inappropriate disclosure of data.
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.	• Guidance on how to provide user-friendly, easy-to-understand disclosures would be useful. This guidance should also evaluate the efficacy and value of AI disclosures in the context of other existing consumer disclosures to reduce confusion or informational overload.
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.	• The Bill should be supported with regulatory guidance to provide illustrative examples of legal and similarly significant effects and parameters for the threshold to be reached. If the right to contest decisions and request review applies to low-risk scenarios and is disconnected from threats to fundamental rights, it risks creating an obligation that providers may struggle to comply with, considering the potential number of users and requests that could materialize.

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.	• This might not be possible in all systems and use cases. Suggest adding "where technically possible".
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;	• The definition of "abusive data" should be clarified.
II – are based on imprecise or statistically unreliable methods; or	• Some technologies, methodologies, and methods mature over time. Accuracy and reliability are incremental, and it is unclear what thresholds will be deemed reasonable.
III – do not adequately consider the individuality and personal characteristics of individuals.	• Additional guidance on the definition of these terms and their intended effect would be useful.
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.	• Higher burdens on AI systems should be limited to high-risk AI systems that produce legal or similarly significant effects on individuals. However, this provision requires clarification as it may address AI systems producing little or no significant effects on individuals, such as the creating of profiles in lower risk contexts, and obliges organizations to provide human intervention accordingly.
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.	• The requirements for correction should be commensurate with the potential risk of the system. As currently worded under this provision, even a low-risk system that cannot provide human review would be required to provide reanalysis irrespective of the burden or the benefit that it would provide.
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.	• Subsequent regulatory guidance should provide a list of illustrative examples and criteria on what constitute an irreversible impact. • Not all decisions that are irreversible pose significant risks to individuals. In fact, many AI systems produce results that are meaningless to reverse precisely because they are so low risk. In these low-risk cases, it is not necessary to require ultimate human determinations.
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:	• It is often necessary to process sensitive forms of personal information (e.g., data on race, ethnicity, gender, etc.) to prevent and detect bias in algorithms. It may be useful to clarify that processing of sensitive personal data is permissible with or without the data subject's consent to ensure these obligations are met, consistent with Article 11 (2)(a) of LGPD, which enables controllers to process sensitive data to ensure compliance with a legal obligation.

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	• As noted above, it is often necessary to process sensitive forms of personal information to prevent and detect bias in algorithms. • This is in line with the proposed EU AI Act which enables the processing of sensitive data under the GDPR to the extent that it is strictly necessary for the purposes of ensuring bias monitoring, detection and correction in relation to high-risk AI systems, subject to appropriate safeguards. • Appropriate risk assessment can determine the proper use of sensitive data to identify and address inappropriate and biased outcomes. • At the same time, it is important to note that some data that are not classified as "sensitive" under existing law may still be associated with higher risks. For example, while Article 5(II) LGPD does not classify gender as sensitive data, data indicating a subject's gender may pose heightened risks that may require commensurate protections and mitigations.
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.	• It is not clear what "registration" refers to here. • The preliminary assessment requirement only addresses suppliers but not operators. It seems to assume that operators will only use AI systems in configurations or for purposes consistent with those specified by the supplier. It would be useful to note that use outside these specifications could introduce different risks that require additional assessment. • For clarity, it should be specified that the preliminary assessment will consist of a simple pre-screening or triage assessment to determine whether a full-scale impact assessment is necessary considering the criteria provided in the law and guidance. This would allow organizations to better allocate their resources to the assessment of AI applications that may carry a high risk and prevent organizations from undertaking assessment of AI use in contexts where it is obvious that there is very little risk involved. • Any requirement for prior consultation with regulators or prior conformity assessments should be limited to only high-risk AI uses where risks cannot be sufficiently mitigated, and residual risks remain high. • The regulation, or regulatory guidance pursuant to the regulation, should provide illustrative criteria to

	organizations for determining risk levels/classifications, especially in determining high-risk AI applications.
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.	• It would be impossible for suppliers to document every conceivable use of an AI system. Instead, the provision should ensure that suppliers clearly document the intended primary uses of the system.
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:	• We recommend creating a list of uses that are “presumptively prohibited,” Organizations that still want to engage in these uses will need to mitigate the risks and obtain approval from the relevant authority, subject to an appropriately robust standard of proof that the benefits to individuals or society substantially outweigh the mitigated risks. • Further guidance, including examples, of prohibited activities would be helpful.
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;	• Prohibitions should not be used lightly and should be carefully constrained to clearly identified categories. “Subliminal techniques” are not defined and require additional clarity if they are to be included.
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;	• The provision in question is imprecise relating to the term "vulnerabilities of specific groups of natural persons" - it is not clear whether the examples provided are intended to be exhaustive or merely illustrative.
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.	• This requires immediate regulatory guidance/clarity for organizations to avoid legal uncertainty. A more suitable approach would be (i) to describe factors, criteria and potential harms that risk assessments should consider; (ii) to provide, at most, an illustrative list of potentially excessive risk uses that can be rebutted in each case; (iii) to provide ongoing guidance on how to assess risks and benefits based on learnings over time.
High Risk	
Art. 17. High-risk artificial intelligence systems are those used for the following purposes:	• Creating pre-determined, categorical lists of what kind of processing activities are always high-risk would result in both overregulating, thereby impeding beneficial processing activities that may not warrant high-risk treatment in a given context, and underregulating, by precluding effective mitigations where high-risk treatment would be warranted. • The framework for identifying covered high-risk AI applications should involve the use of impact assessments designed to assess the likelihood, severity and scale of the impact of the AI use. • The approach for identifying covered "high-risk" AI applications must work for organizations of all sizes. It should not be too complex, prescriptive or multi-layered, which would be disproportionate for most organizations, difficult to apply in practice, and may hamper the development and deployment of innovative AI technologies. • Illustrations of high-risk AI applications provided in the regulation or regulatory guidance should be treated as rebuttable presumptions. This would enable organizations to take account of the highly contextual nature of AI applications and give them the opportunity to demonstrate that the use of an AI application in a specific context does not present a high risk. Such approach, for instance, can be observed in the European Parliament's negotiating mandate regarding the EU AI Act that providers of certain AI systems may rebut the presumption that the system should be considered a high-risk AI system. • In some instances, the benefits of an AI use to individuals, or a group of individuals, may be significant despite its risks. While the benefit of the AI use should not directly affect the risk classification of an AI application, consideration of the benefit would reduce the reticence risk of not going forward with the intended beneficial AI application merely due to the possibility of high risk. A balancing between benefits and risks could be performed. In the context of AI, this requires an organization to weigh the legitimate interests of using an AI technology (for the organization, individuals, groups of individuals, society) against the interests

	or fundamental rights of individuals to ensure both benefits and risks are considered and weighed against each other in the development and implementation of a given AI application.
I – application as safety devices in the management and operation of critical infrastructures, such as traffic control and water and electricity supply networks;	• The concept of "critical infrastructure" needs to be clarified, unless that has a specific meaning in Brazil's legal framework. It is also not clear whether the examples provided are intended to be exhaustive or merely illustrative.
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;	• As mentioned above, the Bill should consider that the level of risk of an AI system depends on the specific circumstances of the AI use case. For instance, AI used for recruitment can be sensitive, but there may be recruitment use cases where the risk is low because there is no appreciable impact on future career prospects and livelihoods. Similarly, AI used for task allocation could be sensitive when it is used to determine the main professional activities of an employee, potentially impacting that employee's future development opportunities. However, there are situations where the use of AI for task allocation does not contain any of the same risks. For instance, an organization may choose to use an AI-based task allocation system to distribute tasks amongst a group of volunteers for short-term assignments (e.g., in another department or region) in addition to their day-to-day job based on the volunteers' respective skills. Such a use does not have an appreciable impact on future career prospects and livelihoods of those persons, but rather matches up the relevant skillsets and interests with the relevant volunteering activities or short-term assignments, freeing up time for resources to be spent on other areas.
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;	• "Biometric identification systems" should be clearly defined in the text, and the Bill should clarify whether it is particularly intended to be distinct from "biometric authentication systems". Biometric identification systems involve the processing of biometrics of an indiscriminate number of individuals and requires

	comparing an individual's biometric data to the biometric data of many other individuals stored in a database to identify said individual (i.e., one-to-many matching). On the other hand, biometric authentication systems may entail less risk, given that it consists of comparing two biometric templates usually assumed to belong to the same individual (i.e., one-to-one matching). However, the risk associated with the biometric application ultimately depends on the architecture of the technology, whether personal data is collected and stored, and whether it takes place at the request or knowledge of an individual. There are additional implications depending on the potential users of biometric applications (e.g., a state actor using identifying technology for surveillance versus an individual user unlocking their smartphone). Thus, it is important for the Bill, in considering the associated risk of biometric identification systems, to take into account the context of biometric application.
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:	• Additional factors to be taken into consideration:
	  • Severity and likelihood of harm to individuals, groups, or society at large (relying on conclusions that can be reached with reasonable certainty);
	  • Level and meaningfulness of human involvement and review and appropriateness given the context;
	  • Magnitude and likelihood of benefit of the AI use for individuals, groups of individuals, or society at large;
	  • Reticence risk and/or opportunity costs of not using the AI for individuals, groups of individuals, or society at large. This would include weighing of benefits of the AI use versus leaving the process under the current status quo (i.e., measuring whether the outcome is enhanced by the use of AI rather than leaving it as currently done); and
	  • Mitigation measures to address the risks.
	• Satisfying a single criterion should not automatically make a system high or excessive risk. Instead, the decision should reflect the consideration of all the relevant criteria listed under Article 18 as well as the potential benefits of the potentially high or excessive risk use.

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;	• It is important to ensure that AI systems are not causing unlawful discrimination or having specific, pernicious negative effects. The language should focus on preventing unlawful discrimination and such effects.
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;	• Criteria will be needed to determine whether one system is similar to another. Moreover, the provision should focus on the contexts in which the systems will be used, not the systems themselves.
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.	• Updating the list of high-risk uses is an important deliberation that should reflect the views of all affected stakeholders, and one that should consider both the risks and benefits of the technology, in addition to related tradeoffs.
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:	• We strongly support the principles in Article 19 – they reflect bedrock concepts of an accountability-based approach to governance of AI systems. They reflect concepts reflected in CIPL's Accountability Framework, which has seven elements: Leadership and Oversight, Risk Assessment, Policies and Procedures, Transparency, Training and Awareness, Monitoring and Verification, and Response and Enforcement. For more information, see CIPL Accountability Mapping Report. • One might incorporate additional elements of the Accountability Framework into the requirements of Article

	19, such as the establishment of internal training and awareness programs. • The regulatory framework should also provide appropriate rewards and encouragements to further stimulate and help accelerate AI accountability and organizational best practices. Such "incentives" could include: linking proof of accountability to external certifications; recognizing self-regulatory commitments of organizations that publicly define the AI values and principles they implement along with progress against benchmarks; using demonstrated accountability as a "license to operate" by allowing accountable and/or certified organizations greater opportunities to use and share data responsibly to facilitate growth in responsible AI uses; allowing broader use of data in AI for socially beneficial projects; using demonstrated AI accountability as a criterion for public procurement projects or B2B due diligence; and recognizing demonstrated AI accountability as a mitigating factor or as a liability reduction factor in the enforcement context.
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.	• The AI lifecycle is complex and involves a variety of actors throughout the process. The Act should make clear that obligations may differ according to the role entities play in the AI lifecycle.
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;	• The Bill should adopt an approach that provides flexibility in format, provided that all required elements are included. • The Bill should not, in all instances, require formally documenting each single decision taken in the development of an AI system. Often, multiple actors interact across multiple phases in the development of an AI system. Even if each single actor documented the decisions taken in their respective lifecycles, it is unlikely these decisions will adequately represent the overall risk level of the system, as the latter will depend on multiple factors, including the context of deployment.
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;	• Harms such as social bias are important to address but sometimes challenging to assess. Parties should be asked to show good faith and reasonable effort, relying on available guidance. Parties should not be penalized for decisions later deemed incorrect for which evaluations were conducted in good faith.
b) composition of an inclusive team responsible for the design and development of the system, guided by the pursuit of diversity.	• Guidance on how diversity and inclusiveness should be measured for the purposes of fulfilling this requirement would be helpful.
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;	• Should add language that recognizes normal ranges of likelihood that errors may occur, e.g., add, "normal margins of error" after "characteristics of the system."
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;	• The proposed terms in this provision require greater clarity and the Bill, or subsequent regulatory guidance, should provide further indications of how the public sector should implement these obligations in practice.
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 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.	• It will be important to make clear the limits of application of the rights and obligations in this Act vs. those to be included in the normative act mentioned here. If any obligations in this Act will *not* apply to public sector entities, this limitation in application should be made explicit. • It is important to enable the processing of data on race, color, ethnicity to the extent it is necessary to identify and prevent discrimination and bias.
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.	• Consider amending paragraph 2 to stipulate that government entities should assess and weigh benefits as well as risks associated with AI systems' development and deployment—and the risks associated with *not* developing and deploying the system—in the context of algorithmic impact assessments.
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.	• The relationship between operators and suppliers should be clarified in terms of their respective roles and responsibilities with respect to impact assessment obligation. It is likely that both will need to do risk/impact assessments to assess the risks that are within their control during the development phase and deployment and use phase, respectively. • The Bill and authorities might clarify that preparing impact assessments in good faith and in compliance with the requirements can serve as a mitigating factor in an enforcement context, which would serve as an additional incentive for providing complete and accurate impact assessments.
Sole Paragraph. The competent authority will be notified of the high-risk system by sharing preliminary and algorithmic impact assessments.	• The Bill should clarify whether all parties developing high-risk systems are required to notify the competent authority, and whether parties need to receive any explicit authorization to proceed with development or deployment. Requiring notice of every proposed high-risk use could create a process that is unnecessarily burdensome for both government and the organizations proposing the AI systems for development or use. • The bill or subsequent guidance might affirm that the disclosure of an algorithmic impact assessment to the competent authority does not constitute a waiver of any attorney-client privilege or work-product protection that might exist with respect to any information contained in the algorithmic impact assessments.
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.	• It is appropriate to require that, where necessary, algorithmic impact assessments be conducted in a manner that complies with industry standard best practices. This provision should not proscribe what those standards are or how entities must meet those standards, as it will likely vary substantially across the industry. For example, larger companies may create in-house processes, while smaller entities may use third party services.

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;	• External, third-party audits can play an important role in any accountability framework, including AI accountability. The bill should set clear criteria for when external audits will be required, such as extremely high-risk cases or demonstrated unwillingness to act responsibly, such as a finding of non-compliance or violation of an earlier enforcement order.
	• Ideally, external audits are conducted by certified entities with a duty to protect public interests and ensure that legal criteria are met. Additionally, public researchers often conduct third-party, external audits to better understand the impact of products and services on certain groups. Again, these audits can help increase trust by demonstrating that an AI application possesses necessary characteristics. Additionally, external audits can provide more robust and neutral views on particularly difficult ethical and compliance issues and may therefore be viewed as more credible by the public. External audit requirements should be designed through consultation with stakeholders and updated regularly based on technological developments and new practices.
	• There are specific challenges associated with external audits of AI models and systems, for compliance with non-binding trustworthy AI goals as well as laws. These include:
	  ◦ Ensuring that deployers provide transparency and notice when deploying AI systems;
	  ◦ Accessing the data that models are trained on; and
	  ◦ Access to pre-deployment internal assessments.
	• In addition, before an AI model is tested for bias, it should be tested for functionality. However, external auditors and researchers often face a "black box" problem and cannot recreate the models to test for functionality because they lack access to the actual datasets that were used to train the model.
	• Whether assessments are mandatory or voluntary, organizations should be given flexibility in how they conduct them so long as they meet certain standards and are producible upon request by regulators.
	• The provider of an AI system is best positioned to determine how to conduct impact assessment and risk mitigation for the AI systems they developed. The regulator should strive to provide an objective and/or standard for the provider to strive to, but it should be up to the provider to choose the best means and processes to comply.

Art. 24. The impact assessment methodology will contain, at least, the following steps:	• While the Bill (or regulatory guidance) should provide impact assessment templates detailing minimum requirements, it should maintain a flexible approach so long as all substantive considerations are included based on the context of the processing. The Bill should also adopt an approach that provides flexibility in format around certain required elements.
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;	• Risks to be recorded should be "reasonably" foreseeable.
b) benefits associated with the artificial intelligence system;	• The requirement to assess benefits as well as risks is commendable. This enables a more complete calculus of potential impact.
c) likelihood of adverse consequences, including the number of people potentially impacted	• The concept of "adverse consequences" should be clarified in the Bill or through further regulatory guidance for the sake of predictability and certainty.
d) severity of adverse consequences, including the effort required to mitigate them;	• See above.
e) operating logic of the artificial intelligence system;	• The authors of the Bill should reconsider whether to include logic of AI systems in impact assessments. Similar logical systems can perform differently depending upon the use of the system, and impact assessments should be technology neutral.
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.	• Any incipient, incomplete, or speculative evidence that is used should be described accordingly. While such evidence can be useful, it can also have limitations that are important to contextualize.
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.	• Because the impact assessment will necessarily be done for a large number of AI systems, and by entities large and small, the criteria should be established with clarity and certainty in advance.
Paragraph 4 It will be up to the competent authority to regulate the periodicity of updating impact assessments, considering	• The Bill (or subsequent regulatory guidance) should specify the periodicity of impact assessments. A reasonable approach could be that a business must submit an impact assessment, preferably in summary

the life cycle of high-risk artificial intelligence systems and the fields of application, and may incorporate best sectoral practices.	form, for processing activities that meet a certain risk-level threshold once and then again in the event of any material changes to the processing, which could include changes in business models, risk, law, technology and other external and internal factors.
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.	• See comments under Article 24(para 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.	• As described in Art. 23, algorithmic impact assessments should be conducted by experts operating consistent with industry standards and best practices.
Art. 26. Industrial and commercial secrets being guaranteed, the conclusions of the impact assessment will be public, containing at least the following information:	• See Comments under Article 22 (solo paragraph)
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	• Comment applicable to Articles 27-29: Adoption of organizational accountability mechanisms by all actors in the AI ecosystem will lead to better compliance and outcomes on the ground, and likely result in less need to resort to questions around liability. • Where questions around liability do arise, apportionment among AI agents can be challenging. For example, if a particular deployment of an AI system results in harm to an individual, should liability be assigned to the developer of the system, the deployer, or some combination, depending on the circumstances of the case? Naturally, the deployer is expected to conduct an impact assessment of the service, but this assessment often relies on the information that the developer has provided to the deployer to be able to assess the model that it is being incorporated into the service to be deployed. Without accurate information, it is often difficult to assess the full range of impacts at the deployer level. In addition, it is worth noting that there are many safeguards that can be implemented upstream to prevent downstream harm.

	• The bill could note that regulators will seek to apportion liability according to parties' share of responsibility for generating the harm in question, while remaining cognizant that contracting practices will also play an important role in shaping and apportioning responsibilities and liabilities.

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.	• The Act should encourage AI system operators to engage in appropriate risk assessment and mitigation efforts. Where operators have acted reasonably and worked to mitigate foreseeable risks, they should only be liable for harm caused through their own negligence. Operators of AI systems should only be held to the highest levels of liability where they are in violation of the act and their systems cause harm.
	
	• For instance, Brazil lawmakers may take proposed measures in the EU into consideration. While liability is not explicitly covered in the EU AI Act, a proposed AI Liability Directive aims to clarify the role of civil liability for damage caused by AI systems in the absence of contractual relationship. Accordingly, Article 4 of the Directive would introduce a rebuttable presumption of causation between the defendant's fault and damage caused by AI systems. This presumption would become applicable subject to the following three conditions:
	  • (i) the claimant has demonstrated that the defendant failed to comply with a duty of care intended to protect against the damage that occurred;
	  • (ii) it can be considered reasonably likely, based on the circumstances of the case, that the fault has influenced the output produced by the AI system or the failure of AI system to produce an output; and
	  • (iii) the claimant has demonstrated that the output produced by the AI system or the failure of the AI system to produce an output gave rise to the damage.

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.	• Please see comment on Civil Liability above. In addition, the Bill should recognize proactive measures taken by organizations in good faith as a mitigating factor in an enforcement context – this will serve as an additional incentive for organizations to carry out risk assessments. • For instance, the proposed AI Liability Directive in the EU establishes a presumption of causality between the fault of the defendant and the output produced by the AI system or the failure of AI system to produce an output. However, in the case of a claim for damages concerning a high-risk AI system, the presumption of causality is not applicable where the defendant demonstrates that sufficient evidence and expertise is reasonably accessible for the claimant to prove the causal link between alleged injury and the actions of the defendant (Article 4(4)). This possibility intends to incentivize defendants to comply with their disclosure obligations, with measures set by the AI Act to ensure a high level of transparency of the AI or with documenting and recording requirements.
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.	• The language here is confusing and leaves unclear whether the burden of proving harms falls to the victim or the agent. • Depending on how it is interpreted, this provision could significantly increase the costs associated with developing and deploying low-risk AI systems, which are quickly becoming widespread and indistinguishable from other logical computational systems.
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.	• We applaud the provisions of Article 30 enabling AI agents to formulate codes of good practice and governance, and the provision stating that participation in such mechanisms will be viewed favorably in enforcement actions. • Additional guidance clarifying how the adherence to the codes will be monitored and enforced would be helpful.
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:	• This might be a translation issue but this is the first time the Bill references to the concept of "developer" – this requires clear definition, especially in the context of allocating the responsibilities and roles of actors in AI life cycle.
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.	• The Act should encourage AI system operators to engage in appropriate risk assessment and mitigation efforts and to participate in the adoption of good practices. Operators should be incentivized to adopt such practices, for instance, by being given a presumption of non-negligence when in full compliance with good practices.
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.	• Globally, many discussions are taking place concerning which regulatory body or bodies should be responsible for AI. Brazil should consider what scope may exist for regulation to be performed by existing regulators. The ANPD will have an important role to play, as many AI applications involve the use of personal data. For cross-cutting issues outside the realm of data protection, such as competition, intellectual property, and anti-discrimination (e.g., for housing and employment), other regulators may be important. In addition, AI use is prevalent in many industry sectors, such as healthcare and financial services, and sectoral regulators will also have an interest in regulation of AI as it pertains to use in their sectors. (Please see *CIPL, AI and Data Protection in Tension* (2018) and CIPL White Paper on Ten Recommendations for Global AI Regulation for discussion of changes in key sectors affected by emerging AI technologies). • Brazil should consider creating a mechanism for regulators to work together through a regulatory hub or other cooperation forum (similar to the UK Digital Regulation Cooperation Forum) to ensure consistent interpretation of AI rules, oversight and enforcement. One might also consider stipulating that this or a separate body serve as a source of expertise and advice to the government and to AI agents on technical topics such as standards, or on specific use cases. The draft EU AI Act contemplates creating a body of this nature (the “Artificial Intelligence Board”). • While each regulator should maintain competence over its own remit (e.g., for purposes of legal certainty, the ANPD should retain general competence over AI applications involving the processing of personal data and/or impacting individuals’ privacy), a standing central governmental coordination body could set high-level AI policies and goals applicable across all sectors and industries, and facilitate alignment, regulatory

	coordination, and joint action between different regulatory bodies, where necessary and appropriate.
Sole Paragraph. It is up to the competent authority to:	• It is unclear whether the competent authority is required to undertake all the activities listed under this paragraph, or if any of them are discretionary. Should "It is up to the competent authority" be interpreted in this context as synonymous with "The competent authority will"?
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.	• Providing for the creation of regulatory sandboxes is a positive aspect of the law. Implementation of this provision should be consistent with the regulatory sandbox initiative announced by ANPD in October 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;	• We commend the inclusion of this mitigation factor, which supports an approach to AI governance grounded in organizational accountability.
IX – the adoption of a policy of good practices and governance;	• We suggest adding that acquiring relevant external certifications should also be a treated as a means of demonstrating a commitment to organizational accountability and a mitigating factor.
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.	• Participation in a sandbox demonstrates commitment to working collaboratively with regulators on responsible deployment of emerging technologies. In recognition of this commitment and to incentivize use of the regulatory sandbox, we recommend that participation in the sandbox be treated as a significant mitigating factor in enforcement actions if the alleged violation relates to an activity that was or is part of the 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.	• We have concerns about the feasibility and advisability of such a database, as noted in our comment on Article 22, Sole Paragraph, above. If the government does establish the database, access should be subject to appropriate safeguards to ensure the confidentiality of personal data and proprietary business information.
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.	