

Provides for the development, promotion and the ethical and responsible use of artificial intelligence based on the centrality of the human person.

The **National Congress** decrees:

CHAPTER I PRELIMINARY PROVISIONS

Art. 1 This Law establishes general national standards for the responsible governance of artificial intelligence (AI) systems in Brazil, with the aim of protecting fundamental rights, stimulating responsible innovation and competitiveness and ensuring the implementation of safe and reliable systems, for the benefit of the human person, the democratic regime and social, scientific, technological and economic development.

§ 1^o This Law does not apply to the AI system:

I – used by a natural person for an exclusively private and non-economic purpose;

II – developed and used solely and exclusively for national defense purposes;

III – used in investigation, research, testing and development activities of AI systems, applications or models before they are placed on the market or put into service, observing the applicable legislation for said activities, in particular Law No. 8,078 of September 11, 1990 (Consumer Defense Code), Law No. 13,709 of August 14, 2018 (General Law on the Protection of Personal Data), Law No. 6,938 of August 31, 1981 (National Environmental Policy), and Law No. 9,610 of February 19, 1998 (Copyright Law), and testing under real conditions must comply with the provisions of this Law;

IV – used in services that are limited to providing infrastructure for storing and transporting data used in AI systems.

§ 2^o In order to promote national technological development, the National System for Regulation and Governance of Artificial Intelligence (SIA) will regulate simplified regimes, involving flexibility of regulatory obligations provided for in this Law, in the following cases:

I – open and free standards and formats, with the exception of those considered to be of high risk;

II – encouraging innovation and scientific and technological research in the production environment, with a view to technological training, achieving technological autonomy and developing the country's national and regional production system;

III – projects of public interest, those that meet the priorities of industrial and science, technology and innovation policies and those that aim to solve Brazilian problems.

Art. 2º The development, implementation and use of AI systems in Brazil are based on:

I – centrality of the human person;

II – respect for and promotion of human rights and democratic values;

III – free development of personality and freedom of expression;

IV – protection of the environment and ecologically balanced development;

V – equality, non-discrimination, plurality and diversity;

VI – social rights, especially the appreciation of human work;

VII – socioeconomic, scientific and technological development and innovation;

VIII – consumer protection, free enterprise and free competition;

IX – privacy, protection of personal data and informational self-determination;

X – promotion of research and development with the purpose of stimulating social development, reducing inequalities and innovation in the productive sectors, in the public sector and public-private partnerships;

XI – access to information and dissemination of data, in an open, structured manner and safe;

XII – protection of cultural rights and promotion of artistic and historical assets;

XIII – education and awareness about AI systems to promote the full development and exercise of citizenship;

XIV – protection and promotion of the rights of vulnerable groups, especially the elderly, people with disabilities and, with full protection and aiming at the best interests, children and adolescents, recognizing their aggravated vulnerability;

XV – integrity of information through the protection and promotion of reliability, accuracy and consistency of information to strengthen freedom of expression, access to information and other fundamental rights;

XVI – strengthening the democratic process and political pluralism;

XVII – protection of copyright and related rights, intellectual property rights and commercial and industrial secrets;

XVIII – guarantee of information security and cybersecurity; XIX – Brazilian insertion, integration and competitiveness in the international market;

XX – international cooperation for the development and compliance with technical standards and national and international obligations.

Art. 3 The development, implementation and use of AI systems shall observe good faith and the following principles:

- I – inclusive growth, sustainable development and well-being, including protection of work and workers;
- II – self-determination and freedom of decision and choice;
- III – effective and adequate human supervision and determination in the AI life cycle, considering the degree of risk involved;
- IV – no unlawful or abusive discrimination;
- V – justice, equity and inclusion;
- VI – transparency and explainability, observing commercial and industrial secrecy, considering the participation of each agent in the AI value chain;
- VII – due diligence and auditability throughout the entire life cycle of the AI system, in accordance with the risk involved and the state of the art of technological development;
- VIII – reliability and robustness of the AI system;
- IX – protection of fundamental rights and guarantees, including due process, contestability and adversarial proceedings;
- X – accountability, responsibility and full compensation for damages;
- XI – prevention, precaution and mitigation of risks and damages;
- XII – non-maleficence and proportionality between the methods employed and the determined and legitimate purposes of the AI system;
- XIII – ethical and responsible development and use of AI;
- XIV – transparent, participatory governance aimed at protecting rights individual, social, collective and economic fundamentals;
- XV – promoting the interoperability of AI systems to enable broader access and collaborative innovation;
- XVI – possibility and condition of using systems and technologies safely and autonomously by people with disabilities, ensuring full accessibility to information and communication;
- XVII – comprehensive protection of children and adolescents.

Art. 4 For the purposes of this Law, the following definitions are adopted:

I – artificial intelligence (AI) system: machine-based system that, with different degrees of autonomy and for explicit or implicit purposes, infers, from a set of data or information it receives, how to generate results, in particular prediction, content, recommendation or decision that may influence the virtual, physical or real environment;

II – life cycle: series of phases, from conception, planning, development, training, retraining, testing, validation, implementation and monitoring, to possible modifications and adaptations of an AI system, the discontinuity of which may occur at any of the aforementioned stages;

III – general purpose artificial intelligence system (PGAIS): AI system based on an AI model trained with large-scale databases, capable of performing a wide variety of different tasks and serving different purposes, including those for

which were not specifically developed and trained, and can be integrated into different systems or applications;

IV – generative artificial intelligence (generative AI): AI model specifically designed to generate or significantly modify, with different degrees of autonomy, text, images, audio, video or **software code**;

V – developer: a natural or legal person, whether public or private, who develops an AI system, directly or by order, with a view to placing it on the market or applying it to a service provided by it, under its own name or brand, whether for a fee or free of charge;

VI – distributor: natural or legal person, of a public or private nature, who makes available and distributes an AI system for third parties to apply, whether for a fee or free of charge;

VII – applicator: natural or legal person, of a public or private nature, who employs or uses, in his/her name or benefit, an AI system, including configuring, maintaining or supporting with the provision of data for the operation and monitoring of the AI system;

VIII – artificial intelligence agents: developers, distributors and applicators who operate in the value chain and internal governance of AI systems, under the terms defined by regulation;

IX – competent authority: federal public administration entity, endowed with technical and decision-making autonomy, which will coordinate the National Regulatory and Artificial Intelligence Governance (AIS);

X – National System for Regulation and Governance of Artificial Intelligence (SIA): regulatory ecosystem coordinated by the competent authority whose main purpose is to promote and guarantee cooperation and harmonization with other sectoral authorities and regulatory bodies, without any hierarchical subordination link between them, and other national systems for the full implementation and monitoring of compliance with this Law throughout the national territory, with legal certainty;

XI – abusive or unlawful discrimination: any distinction, exclusion, restriction or preference, in any area of public or private life, the purpose or effect of which is to nullify or restrict, in an abusive or unlawful manner, the recognition, enjoyment or exercise, under conditions of equality, of one or more rights or freedoms provided for in the legal system, on the basis of personal characteristics;

XII – abusive or unlawful indirect discrimination: discrimination that occurs when a seemingly neutral rule, practice or criterion has the capacity to cause disadvantage to the person or groups affected, or place them at a disadvantage, provided that this rule, practice or criterion is abusive or unlawful;

XIII – text and data mining: process of extracting and analyzing large amounts of data, with a high degree of automation, carried out directly on primary data, or indirectly through another tool, from which patterns and correlations are extracted that will generate relevant information for research, development or use of AI systems;

XIV – affected person or group: natural person or group of people who are directly or indirectly impacted by an AI system;

XV – preliminary assessment: simplified self-assessment process, prior to the use or placing on the market of one or more AI systems, to classify their degree of risk, with the aim of determining compliance with the obligations defined in this Law;

XVI – algorithmic impact assessment: analysis of the impact on fundamental rights, presenting preventive, mitigating and reversal measures for negative impacts, as well as measures to enhance the positive impacts of an AI system;

XVII – vulnerability: state of aggravated asymmetry of information or power that affects individuals or groups due to, among others, their cognitive, social, ethnic, economic and age conditions, such as children and adolescents, the elderly and people with disabilities;

XVIII – experimental regulatory environment (**regulatory sandbox**): set of special conditions established to develop, train, validate and test, for a limited time, an innovative AI system, as well as innovative business models and public policies and experimental techniques and technologies involving AI, by complying with previously established criteria and limits and through a simplified procedure;

XIX – state of the art of technological development: reasonable technical means and available, based on scientific and technological evidence and consolidated good practices;

XX – relevant legal effects: modifying legal consequences, negative impediments or extinguishments that affect fundamental rights and freedoms;

XXI – synthetic content: information, such as images, videos, audio and text, that have been significantly modified or generated by AI systems;

XXII – integrity of information: the result of an information ecosystem that enables and makes available reliable, diverse and accurate information and knowledge, in a timely manner to promote freedom of expression;

XXIII – biometric identification: method that involves the recognition of human physical, physiological and behavioral characteristics, with the purpose of identifying an individual;

XXIV – biometric authentication: process of verifying or confirming an individual's identity, with the aim of uniqueizing them, by comparing their biometric characteristics obtained from a previously stored model;

XXV – introduction or placing into circulation on the market: availability initial or introduction for users of the AI system, whether paid or free of charge;

XXVI – sectoral authorities: bodies and entities of the federal Executive Branch responsible for regulating specific sectors of economic and governmental activity, in accordance with their legal competence;

XXVII – autonomous weapons systems (AWS): systems that, once activated, can select and attack targets without additional human intervention;

XXVIII – application programming interface (API): set of protocols and functions that allow different systems to interact with each other;

XXIX – context of use: specific use for which the AI system or application is intended, including the system to be used, the specific context and purpose and its conditions of use;

XXX – systemic risk: potential negative adverse effects arising from a general-purpose and generative AI system with a significant impact on individual and social fundamental rights.

CHAPTER II OF RIGHTS

Section I

Rights of the Person or Group Affected by an AI System

Art. 5 The person or group affected by an AI system, regardless of its degree of risk, has the following rights, to be exercised in the manner and under the conditions described in this Chapter:

I – right to information regarding their interactions with AI systems, in an accessible, free and easy-to-understand manner, including regarding the automated nature of the interaction, except in cases where the AI systems are dedicated solely and exclusively to cybersecurity and cyberdefense, as per regulation;

II – right to privacy and protection of personal data, in particular the rights of data subjects under Law No. 13,709 of August 14, 2018 (General Law on the Protection of Personal Data) and relevant legislation;

III – right to non-unlawful or abusive discrimination and to the correction of unlawful or abusive discriminatory biases, whether direct or indirect.

§ 1^o The information referred to in item I of the **caput** of this article will be provided using easily recognizable standardized icons or symbols, without prejudice to other formats.

§ 2 AI systems intended for vulnerable groups must, at all stages of their life cycle, be transparent and adopt simple, clear language appropriate to their age and cognitive capacity, and be implemented considering the best interests of these groups.
groups.

Section II

Rights of the Person or Group Affected by a High-Risk AI System

Art. 6 The person or group affected by a high-risk AI system has the following rights:

I – right to an explanation of the decision, recommendation or forecast made by the system;

II – the right to challenge and request a review of decisions, recommendations or AI system predictions;

III – right to human review of decisions, taking into account the context, risk and state of the art of technological development.

§ 1^o The explanation referred to in item I of the **caput** of this article, respecting commercial and industrial secrecy, will include sufficient, adequate and intelligible information, in accordance with the regulations.

§ 2 The rights provided for in this Section will be implemented considering the state of the art of technological development, and the agent of the high-risk AI system must always implement effective and proportionate measures.

Art. 7 The right to explanation provided for in this Section will be provided through a free process, in simple, accessible and appropriate language that facilitates the person to understand the result of the decision or prediction in question, within a reasonable period of time, depending on the complexity of the AI system and the number of agents involved.

Sole paragraph. The competent authority shall regulate deadlines and procedures for exercising the right to explanation, including a simplified procedure, considering, among others, the following criteria:

I – the complexity of AI systems;

II – the size of the agent, especially in the case of micro and small companies and

startups.

Art. 8 Human supervision of high-risk AI systems will seek to prevent or minimize risks to the rights and freedoms of affected individuals or groups that may arise from their normal use or from their use under reasonably foreseeable conditions of misuse, enabling those responsible for human supervision to, under the terms of the regulation, understand, interpret, decide and intervene in AI systems, as well as prioritize the management of risks and irreversible impacts.

Sole paragraph. Human supervision shall not be required if its implementation is demonstrably impossible or involves disproportionate effort, in which cases the agent of the high-risk AI system shall implement effective alternative measures.

Art. 9 High-risk AI agents shall inform, in a sufficient, objective, clear and accessible manner, the procedures necessary for exercising the rights described in this Chapter.

Art. 10. The competent authority shall establish, where applicable and always in formal institutional cooperation with the SIA sectoral authorities, general guidelines on the form and conditions for exercising rights before each of the AI system agents.

Art. 11. The defense of the interests and rights provided for in this Law may be exercised:

I – before the competent administrative body;

II – in court, individually or collectively, in accordance with the provisions of the relevant legislation regarding individual, collective and diffuse protection instruments.

CHAPTER III RISK CATEGORIZATION

Section I

From the Preliminary Assessment

Art. 12. Before its introduction and circulation in the market, employment or use, the AI agent may carry out a preliminary assessment to determine the degree of risk of the system, based on the criteria provided for in this Chapter, in accordance with the state of the art of technological development.

§ 1^o Carrying out the preliminary assessment will be considered as a good practice measure and may result in benefits for the AI agent for the purposes of the provisions of art. 50, § 1, and may even receive priority treatment in procedures for conformity assessment, under the terms of art. 34, both of this Law.

§ 2^o It will be up to the sectoral authority to define the cases in which the preliminary assessment will be simplified or waived, in compliance with the general rules of the competent authority.

§ 3 The agent may request from other agents of the AI systems information that enables it to carry out a preliminary assessment, in accordance with this Law, respecting commercial and industrial secrets.

§ 4^o Once the adversarial system and full defense are guaranteed, the competent authority may, in collaboration with the SIA sectoral authorities, determine the reclassification of the AI system, upon prior notification, as well as determine, in a reasoned manner, the performance of an algorithmic impact assessment.

§ 5 The result of the preliminary assessment may be used by the AI agent to demonstrate compliance with the security, transparency and ethics requirements set forth in this Law.

§ 6 The sectoral authority may request the performance of or access to the preliminary assessment of the AI system for the purposes of assessing the system's risk, respecting commercial and industrial secrets.

Section II

Of Excessive Risk

Art. 13. The development, implementation and use of information systems are prohibited.

AI:

I – for the purpose of:

- a) instigate or induce the behavior of a natural person or groups in a way that causes harm to their own health, safety or other fundamental rights or those of third parties;
- b) exploit any vulnerabilities of the natural person or groups with the aim or effect of inducing their behaviour in a way that causes harm to their own health, safety or other fundamental rights or those of third parties;
- c) assess the personality traits, characteristics or past behavior, criminal or otherwise, of individuals or groups, to assess the risk of committing crimes, infractions or reoffending;

d) enable the production or dissemination or facilitate the creation of material that characterizes or represents sexual abuse or exploitation of children and adolescents;

II – by the public authorities, 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, in an illegitimate or disproportionate manner;

III – in autonomous weapons systems (AWS);

IV – in remote biometric identification systems, in real time and in spaces accessible to the public, with the exception of the following hypotheses:

a) instruction of an inquiry or criminal proceedings, with prior and reasoned judicial authorization, when there is reasonable evidence of authorship or participation in a criminal offense, the evidence cannot be provided by other available means and the fact investigated does not constitute a criminal offense of lesser potential harm;

b) search for victims of crimes and missing persons, or in circumstances involving a serious and imminent threat to the life or physical integrity of natural persons;

c) flagrant offence of crimes punishable by a custodial sentence of more than 2 (two) years, with immediate communication to the judicial authority;

d) recapture of escaped defendants and enforcement of arrest warrants and restrictive measures ordered by the Judiciary.

§ 1º Developers of AI systems must adopt measures to prevent the use of their systems for the purposes described in the **caput** of this article.

§ 2º The use of systems referred to in item IV of this article must be proportional and strictly necessary to serve the public interest, observing due process and judicial control, as well as the principles and rights provided for in this Law and, where applicable, in Law No. 13,709, of August 14, 2018 (General Law on the Protection of Personal Data), especially the guarantee against discrimination and the need for review of algorithmic inference by the responsible public agent.

Section III **High Risk**

Art. 14. AI systems used for the following purposes and contexts of use are considered high risk, taking into account the probability and severity of adverse impacts on affected individuals or groups, in accordance with regulations:

I – application as security devices in the management and operation of critical infrastructures, such as traffic control and water and electricity supply networks, when there is a significant risk to the physical integrity of people and the interruption of essential services, in an illicit or abusive manner, and provided that they are decisive for the result or decision, operation or access to essential service;

II – AI systems used as a determining factor in decision-making for the selection of students in admission processes to educational or professional training institutions, or for decisive assessments in academic progress or monitoring of

students, except in cases of monitoring exclusively for security purposes;

III – recruitment, screening, filtering or evaluation of candidates, decision-making on promotions or termination of employment contracts, assessment of the performance and behavior of those affected in the areas of employment, management of workers and access to self-employment;

IV – assessment of criteria for access, eligibility, granting, review, reduction or revocation of private and public services that are considered essential, including systems used to assess the eligibility of natural persons for the provision of public assistance and security services;

V – evaluation and classification of calls or determination of priorities for essential public services, such as fire services and medical care;

VI – administration of justice, with regard to the use of systems that assist judicial authorities in investigating facts and applying the law when there is a risk to individual freedoms and the democratic rule of law, excluding systems that assist administrative acts and activities;

VII – autonomous vehicles in public spaces, when their use may generate a significant risk to the physical integrity of people;

VIII – applications in the health area to assist diagnoses and procedures doctors, when there is a significant risk to people's physical and mental integrity;

IX – analytical study of crimes involving natural persons, allowing police authorities to search large data sets, available in different data sources or in different formats, in order to identify behavioral patterns and profiles;

X – investigation by administrative authorities to assess the credibility of evidence in the course of the investigation or prosecution of offences, to predict the occurrence or recurrence of an actual or potential offence based on the profiling of natural persons;

XI – biometric identification and authentication systems for the recognition of emotions, excluding biometric authentication systems whose sole purpose is the confirmation of a specific individual; XII – immigration

management and border control to assess the entry of a person or group of people into national territory.

Sole paragraph. High-risk use is not considered to be that in which the AI system is used as an intermediate technology that does not influence or determine the result or decision or when it performs a restricted procedural task.

Art. 15. The SIA will be responsible for regulating the classification of the list of high-risk AI systems, as well as identifying new high-risk application hypotheses, taking into account the probability and severity of adverse impacts on affected people or groups, and based on at least 1 (one) of the following criteria:

I – the system produces, in an illicit or abusive manner, relevant legal effects and negatively impacts access to public or essential services;

II – high potential for material or moral damage, as well as bias unlawful or abusive discriminatory;

III – the system significantly affects people in a vulnerable group;

IV – degree of reversibility of damage;

V – damaging history, of a relevant material or moral nature;

VI – degree of transparency, explainability and auditability of the AI system that significantly hinder its control or supervision;

VII – high potential for systemic damage, such as to cybersecurity, and violence against vulnerable groups;

VIII – extent and probability of the risks of the AI system, including the mitigation measures adopted and considering the expected benefits, in accordance with the principles and foundations of this Law;

IX – the system poses significant risks to integral human health – physical, mental and social – in the individual and collective dimensions;

X – the system may negatively impact the development and physical, psychological or moral integrity of children and adolescents.

Art. 16. The regulation of the list and classification of new applications of high-risk AI systems will be preceded by a procedure that guarantees social participation and regulatory impact analysis, including:

I – the competent authority, as coordinator of the SIA, must ensure the harmonious application of this Law, and must:

(a) issue general normative guidance on the impacts of AI systems on fundamental rights and freedoms or that produce relevant legal effects;

b) publish the consolidated list of all high-risk systems defined by the sectoral authorities;

II – sectoral authorities, within the scope of their attributions and on a prevailing basis, shall provide for the technical and specific aspects of AI applications in the regulated market, and must:

a) establish lists of hypotheses classified or not classified as high risk within the purposes and contexts defined in art. 14;

b) establish, precisely, the list of high-risk systems under this Law;

c) receive and analyze algorithmic impact assessments;

d) indicate, in a list, cases of use of high-risk or non-high-risk AI systems or applications.

§ 1 The competent authority and sectoral authorities shall consider the state of the art of technological development and the evolution and harmonization of sectoral and non-sectoral good practices for the purposes of monitoring and continuous reclassification of high-risk AI systems.

§ 2 The developer and the applicator who considers that the AI system does not fall within the high-risk classification may submit a substantiated petition to the sector authorities together with their preliminary assessment, in accordance with the regulations.

§ 3 Distributors must ensure that the AI system complies with the measures governance procedures provided for in this Law before being placed on the market.

§ 4 The competent authority and sectoral authorities may accredit conformity assessment bodies that offer AI agents risk identification and classification services for the use of AI systems, in accordance with applicable national and international technical standards.

§ 5 In the classification of new applications of high-risk AI systems, sectoral authorities should:

I – expressly indicate its legal and administrative consequences and the conditions for regularization to occur in a proportional and equitable manner, without imposing on the affected parties burdens or losses that, due to the peculiarities of the case, are abnormal or excessive;

II – consider the real obstacles and difficulties of AI agents and the demands of public policies under their responsibility, without prejudice to the rights of the people and groups affected;

III – provide for a transitional regime so that new obligations and duties are fulfilled in a proportional, equitable and efficient manner and without prejudice to the interests of people and groups affected by AI systems.

§ 6^o The procedure referred to in the **caput** of this article must provide the opportunity for manifestation of the affected productive economic sectors.

CHAPTER IV

ON THE GOVERNANCE OF ARTIFICIAL INTELLIGENCE SYSTEMS

Section I

General Provisions

Art. 17. AI agents must ensure the security of the systems and the fulfillment of the rights of affected individuals or groups, in accordance with regulations.

Section II

Governance Measures for High-Risk Systems

Art. 18. In addition to complying with the provisions of Section I of this Chapter, the developer and the applicant, when introducing or placing into circulation on the market a high-risk system, shall adopt, among others, the following governance measures and the following internal processes, in accordance with the state of the art of technological development and with reasonable efforts:

I – for the applicator:

a) documentation in an appropriate format, considering all relevant steps in the system life cycle;

b) use of tools or processes for the results of using the system, in order to allow the assessment of its accuracy and robustness and to determine potential results

unlawful or abusive discriminatory practices, and implementation of the risk mitigation measures adopted;

c) documentation of testing to assess appropriate levels of reliability and security;

d) documentation in an appropriate format of the degree of human supervision that has contributed to the results presented by the AI systems;

e) measures to mitigate and prevent discriminatory biases, when the risk to discrimination arising from the application of the AI system;

f) provision of adequate information that allows, respecting industrial and commercial confidentiality in accordance with their technical capabilities, the interpretation of results and the operation of AI systems introduced or placed into circulation on the market;

II – for the developer:

a) maintaining a record of the governance measures adopted in the development of the AI system, to provide the necessary information to the applicant so that the latter complies with the obligations determined in item I of the **caput** of this article, in accordance with the legal relationship established between the parties and subject to commercial and industrial confidentiality;

b) use of tools or processes to record the system's operation, in order to allow the assessment of its accuracy and robustness;

c) carrying out tests to assess appropriate levels of security;

d) adoption of technical measures to enable the applicability of the results of AI systems and the provision of adequate information that allows the interpretation of their results and their functioning, respecting industrial and commercial confidentiality;

e) measures to mitigate and prevent discriminatory biases, when the risk to discrimination arising from the application of the AI system;

f) transparency on management and governance policies to promote social and sustainable responsibility within the scope of its activities.

§ 1^o It will be up to the sectoral authorities to define the cases in which the obligations established in the regulation will be made more flexible or waived, according to the context of the AI agent's actions in the AI system's value chain.

§ 2 Distributors must support and verify whether the AI system complies with the governance measures provided for in this Law, before the system is placed into circulation on the market, in accordance with the regulations.

§ 3 The agents in the AI system or application value chain must cooperate with each other, making available the necessary information and providing the technical access and assistance reasonably expected and necessary to fulfill the obligations established in this article, safeguarding industrial and commercial confidentiality.

§ 4 The governance measures and internal processes provided for in this article, to be adopted by the agents, must correspond to the respective phase of the life cycle of the AI system that is their responsibility, in accordance with the level of knowledge about the respective design, implementation, application and use.

§ 5 If the applicator or distributor makes a substantial modification or alters the purpose of an AI system, will be considered a developer for the purposes of this Law.

Art. 19. When the AI system generates synthetic content, it must, considering the state of the art of technological development and the context of use, include an identifier in such content to verify its authenticity or characteristics of its origin, modifications or transmission, as per the regulation.

§ 1º The presence of the identifier provided for in the **caput** does not satisfy other information and transparency requirements, as well as other parameters to be defined in regulation.

§ 2º The competent authority, in collaboration with the Permanent Council for Regulatory Cooperation on Artificial Intelligence (Cria), will make available a **software** library with a view to facilitating compliance with the signaling obligation, ideally adopting a widely recognized international standard.

§ 3º The use of synthetic content in works with artistic, cultural or entertainment purposes may, whenever it does not represent a risk of disseminating false information, be signaled by means that do not compromise the usefulness and quality of the work, such as in the credits or metadata associated with such work, preserving its enjoyment by the public and its conventional uses.

Art. 20. In order to seek to mitigate risks related to the production and circulation of synthetic content, the public authorities, together with the private sector, civil society and research and development professionals, must, in the form of regulation, promote capabilities to identify and label synthetic content produced by AI systems and establish the authenticity and provenance of the digital content produced.

Art. 21. High-risk AI agents must ensure that their systems comply with the governance measures defined throughout Chapter IV of this Law, as well as in other relevant legislation, particularly in their respective sector.

Section III

Governance Measures Applied by Public Authorities

Art. 22. When developing, contracting or adopting high-risk AI systems, the public authorities must guarantee:

I – access to databases and full portability of data of Brazilian citizens and public management, under Law No. 13,709, of August 14, 2018 (General Law on the Protection of Personal Data);

II – the minimum standardization of systems in terms of their data architecture and metadata, in order to promote interoperability between systems and good data governance.

Art. 23. In addition to the governance measures established in this Chapter, all entities of the direct and indirect Public Administration, when developing or using high-risk AI systems, shall adopt the following measures:

I – definition of access and system usage protocols that allow the record of who used it, for what specific situation and for what purpose;

II – facilitated and effective guarantee to citizens, before public authorities, of the right to human explanation and review of decisions made by AI systems that generate relevant legal effects or that significantly impact the interests of the affected party, to be promoted by the competent public agent;

III – publication in easily accessible vehicles, preferably on their websites, of preliminary assessments of high-risk AI systems developed, implemented or used by the public authorities of the Union, the States, the Federal District and of the Municipalities.

§ 1^o The use of biometric systems for identification purposes must observe the principles and governance measures provided for in this Law and will be preceded by an algorithmic impact assessment, observing the guarantees for the exercise of the rights of affected individuals or groups and protection against direct, indirect, illegal or abusive discrimination.

§ 2^o If it is impossible to eliminate or substantially mitigate the risks associated with the AI system identified in the algorithmic impact assessment provided for in Section IV of this Chapter, its use will be discontinued.

§ 3 The measures provided for in this article also apply to AI systems used by companies responsible for managing or executing public services.

§ 4 High-risk AI systems already implemented by the public authorities at the time of publication of this Law must adapt within a reasonable period of time, to be defined by the competent authority.

§ 5 The provisions set forth in the **caput** of this article cover bodies of the Legislative and Judicial Branches, when performing administrative functions, and legal entities under private law responsible for the management or execution of public services, when affected by these activities.

Art. 24. The federal Executive Branch will be responsible for establishing minimum transparency standards for AI systems used by federal public sector bodies and entities, in addition to regularly monitoring compliance with these obligations.

Sole paragraph. The federal Executive Branch shall promote transparency in AI systems used by public bodies and entities with a view to promoting and consolidating responsible and open governance practices.

Section IV **From Algorithmic Impact Assessment**

Art. 25. The assessment of the algorithmic impact of AI systems is the obligation of the developer or user who introduces or places an AI system into circulation on the market, whenever the system or its use is high risk, considering the role and participation of the agent in the chain.

§ 1 The developer of a high-risk AI system must, under the terms of the regulation, share with the sector authority the preliminary and algorithmic impact assessments, the methodology of which will consider and record, at least, an assessment of the risks and

benefits to fundamental rights, mitigation measures and effectiveness of these management measures.

§ 2º The AI agent may request from other agents in the chain, respecting industrial and commercial secrets, the information necessary to carry out the algorithmic impact assessment.

§ 3 The assessment must be carried out at an early stage and in accordance with the specific context of the introduction or placing into circulation on the market of the AI system.

§ 4 The sectoral authority will be responsible for defining the cases in which the algorithmic impact assessment will be made more flexible, taking into account the context of action and the role of each AI agent and the general rules of the competent authority.

§ 5º The competent authority, based on the Cria guidelines, will establish general criteria and elements for the preparation of an algorithmic impact assessment and the frequency of its updating, considering the life cycle of high-risk AI systems.

§ 6 The sectoral authority will be responsible, based on the state of the art of technological development and best practices, for regulating the criteria and frequency of updating algorithmic impact assessments, considering the life cycle of high-risk AI systems.

§ 7 AI agents who, after the introduction of an AI system into the market or its use in service, become aware of an unexpected and relevant risk or impact that the system presents to the rights of natural persons shall immediately communicate the fact to the sectoral authority and to other agents in the chain so that all appropriate measures can be taken, including, when necessary, notifying individuals and groups affected by the AI system.

§ 8º It will be up to the competent authority and the sectoral authorities to establish the cases in which public participation will be necessary, as well as the cases in which it can be carried out in a simplified manner, indicating the criteria for such participation.

Art. 26. The algorithmic impact assessment will be carried out prior to the introduction or placing into circulation on the market of an AI system, and will consist of a continuous interactive process, carried out throughout the entire life cycle of high-risk AI systems, with periodic updates required.

Sole paragraph. Considering any existing sectoral regulations, it will be appropriate the competent authority, in collaboration with the other SIA entities, to define:

I – general parameters regarding the frequency of updating algorithmic impact assessments, which must be carried out at least when there are significant changes to the systems, in accordance with the regulations;

II – the hypotheses in which the algorithmic impact assessment will be simplified, considering the type of AI system agents.

Art. 27. If the AI agent has to prepare a report on the impact on the protection of personal data, in accordance with Law No. 13,709 of August 14, 2018 (General Law on the Protection of Personal Data), the algorithmic impact assessment may be carried out in conjunction with said document.

Art. 28. The conclusions of the algorithmic impact assessment will be public, observing industrial and commercial secrets, in accordance with regulations.

Section V

From Governance Measures to Purpose-Driven Artificial Intelligence Systems General and Generative

Art. 29. The developer of general-purpose and generative AI systems must carry out, in addition to the relevant documentation on the development of the system, its preliminary assessment, in order to identify its respective expected risk levels, including potential systemic risk.

Sole paragraph. The preliminary assessment must consider the reasonably expected purposes of use and the criteria provided for, in accordance with Section III of Chapter III of this Law.

Art. 30. The developer of general-purpose and generative AI systems with systemic risk must, before making them available or introducing them into the market for commercial purposes, ensure compliance with the following requirements:

- I – describe the general-purpose AI model;
- II – document the tests and analyses carried out, in order to identify and manage reasonably foreseeable risks, as appropriate and technically feasible;
- III – document the remaining unmitigable risks after development;
- IV – process and incorporate only data sets collected and processed in compliance with legal requirements and subject to adequate data governance, especially when dealing with personal data, in accordance with Law No. 13,709, of August 14, 2018 (General Law on the Protection of Personal Data) and Chapter II of this Law;
- V – publish a summary of the data set used in training the system, in accordance with regulations;
- VI – design and develop general-purpose and generative AI systems using applicable standards to, considering the context of use, reduce energy use, resource use and waste, as well as to increase energy efficiency and the overall efficiency of the system; VII – prepare intelligible technical documentation and user instructions in order to allow developers, distributors and users to have clarity about how the system works.

§ 1º Compliance with the requirements established in this article is independent of whether the system is provided as a stand-alone model or incorporated into another AI system or product, or provided under free and open source licenses, as a service, as well as through other distribution channels.

§ 2 Developers of general-purpose and generative AI systems may formulate codes of good practice, or adhere to them, to demonstrate compliance with the obligations stipulated in this article.

Art. 32. Developers of general-purpose and generative AI systems made available as a resource for the development of services by third parties, such as those provided through API or other integration models, must cooperate, to the extent of their participation, with other AI agents throughout the period in which this service is provided and supported, in order to allow adequate mitigation of risks and compliance with the rights established in this Law.

Art. 33. It will be up to the competent authority, in collaboration with the other SIA entities, to define in which cases the obligations provided for in this Section will be simplified or waived, according to the risk involved and the state of the art of technological development.

Sole paragraph. The provisions of Chapter VI shall apply, where applicable, and the competent authority shall be responsible for approving codes of conduct and self-regulation for general-purpose AI systems.

Section VI

Accreditation, Certification and Conformity Assessment

Art. 34. The competent authority and sectoral authorities may accredit national or international conformity assessment bodies specialized in AI systems governance to assess compliance with the governance measures and internal processes required by regulatory bodies.

§ 1^o The SIA must establish the validity period of the accreditation and the requirements for its renewal, in accordance with applicable national and international technical standards.

§ 2^o The assessment of the conformity of the use of AI systems must adopt an efficient procedure that is compatible with market dynamics, without compromising the quality and reliability of the process.

§ 3 The general criteria for accreditation of conformity assessment bodies must be established by the competent authority, and the specific criteria, together with the sectoral authorities, in line with international technical standards and considering the specificities of AI systems.

§ 4 The competent authority shall maintain a public and up-to-date register of accredited conformity assessment bodies, including the scope of their accreditation.

§ 5 Accredited conformity assessment bodies will be subject to continuous monitoring and periodic reassessments to ensure the maintenance of their technical competence and compliance with accreditation requirements.

§ 6^o The conformity assessment may be carried out at different levels, considering the complexity and potential risk of AI systems, as defined in specific regulations.

§ 7^o The competent authority and the sectoral authorities may, jointly, establish cooperation and mutual recognition agreements with

international accreditation, aiming to facilitate the recognition of conformity assessments carried out in other countries.

CHAPTER V CIVIL LIABILITY

Art. 35. Civil liability arising from damages caused by AI systems in the context of consumer relations remains subject to the liability rules provided for in Law No. 8,078 of September 11, 1990 (Consumer Defense Code), and in the relevant legislation, without prejudice to the application of the other rules of this Law.

Art. 36. Civil liability arising from damages caused by AI systems exploited, employed or used by AI agents remains subject to the liability rules provided for in Law No. 10,406 of January 10, 2002 (Civil Code), and in special legislation, without prejudice to the application of the other rules of this Law.

Sole paragraph. The definition, in concrete terms, of the civil liability regime applicable to damages caused by AI systems must take into account the following criteria, unless otherwise provided by law:

I – the level of autonomy of the AI system and its degree of risk, in accordance with governed by this Law;

II – the nature of the agents involved and the consequent existence of a specific civil liability regime in the legislation.

Art. 37. The judge will reverse the burden of proof when the victim is underprivileged or when the operating characteristics of the AI system make it excessively onerous for the victim to prove the requirements of civil liability.

Art. 38. Participants in the AI regulatory testing environment remain liable under applicable law for any damages inflicted on third parties as a result of experimentation taking place in the testing environment.

Art. 39. The hypotheses of liability provided for by specific legislation remain in force.

CHAPTER VI GOOD PRACTICES AND GOVERNANCE

Section I From the Code of Conduct

Art. 40. AI agents may, individually or through associations, formulate codes of good practice and governance that establish the conditions of organization, the operating regime, the procedures, including regarding complaints from affected persons, the safety standards, the technical standards, the specific obligations for each sectoral context of implementation, the educational actions, the internal mechanisms of

supervision and risk mitigation measures and the appropriate technical and organizational security measures for managing the risks arising from the application of AI systems in their respective field of activity.

§ 1º When establishing good practice rules, the purpose, probability and severity of the risks and benefits arising from the application of AI systems and the possible impacts on vulnerable groups will be considered, following the example of the methodology set out in Section IV of Chapter IV.

§ 2 Developers and users of AI systems may implement a governance program that, in accordance with the state of the art of technological development:

I – demonstrate your commitment to adopting internal processes and policies that ensure comprehensive compliance with standards and good practices regarding non-maleficence and proportionality between the methods employed and the determined and legitimate purposes of AI systems;

II – be adapted to the structure, scale and volume of its operations, as well as its potential for harm and benefits;

III – has the objective of establishing a relationship of trust with affected individuals and groups, through transparent action that ensures participation mechanisms, as provided for in Section IV of Chapter IV of this Law;

IV – is integrated into its general governance structure and establishes and applies internal and external supervision mechanisms;

V – have response plans to reverse possible harmful results of the AI system;

VI – be constantly updated based on information obtained from continuous monitoring and periodic assessments;

VII – have internal mechanisms and procedures for integrity, auditing, encouraging the reporting of irregularities and effective application of codes of ethics.

§ 3 Voluntary adherence to a code of good practices and the development of governance measures may be considered an indication of good faith on the part of the agent and will be taken into account into consideration by the competent authority and other sectoral authorities for the purposes of applying administrative sanctions.

§ 4º It is the responsibility of the sectoral authorities:

I – approve codes of good conduct regarding the sphere of competence granted by law, and must always inform the competent authority;

II – observe the general guidelines and standards for the procedure of analysis, publication and periodic updating of the code of conduct issued by the competent authority.

Section II

Self-regulation

Art. 41. AI agents may voluntarily associate in the form of a non-profit private legal entity to promote self-regulation with the aim of encouraging and ensuring best governance practices throughout the entire life cycle of AI systems.

§ 1^o Self-regulation may include the following functions:

I – establishment of technical criteria for applied AI systems, including standardization, prudential criteria and concerted action by associated entities, provided that they do not impede technological development and are in compliance with this Law and the binding rules of the SIA;

II – sharing experiences on the use of AI, with the sharing of competitively sensitive information being prohibited, in accordance with the relevant legislation;

III – contextual definition of governance structures provided for in this Law;

IV – criteria for invoking the competent authority and other authorities members of the SIA for the use of precautionary measures;

V – creation of a channel for receiving relevant information about the risks of using AI by its members or any interested party;

VI – adoption of internationally recognized standards, best practices and certification models.

§ 2^o The association between AI agents for self-regulation purposes must observe the precepts of Law No. 12,529, of November 30, 2011 (Competition Defense Law), prohibiting any action that may restrict free competition.

CHAPTER VII REPORTING A SERIOUS INCIDENT

Art. 42. The AI agent shall communicate, within a period to be established, to the sector authority the occurrence of a serious security incident, including when there is a risk to the life and physical integrity of people, the interruption of the functioning of critical infrastructure operations and serious damage to property or the environment, as well as serious violations of fundamental rights, the integrity of information, freedom of expression and the democratic process, in accordance with the regulations.

§ 1^o Communication will be due after the sector authority defines the deadline and criteria for determining the severity of the incident, taking into account the characteristics of AI systems in accordance with the state of the art of technological development.

§ 2 The sector authority will verify the severity of the incident and may, if necessary, order the agent to adopt measures and arrangements to reverse or mitigate the effects of the incident.

Art. 43. AI agents, in addition to the provisions of this Law, remain subject to specific legislation relating to cybersecurity and the protection of critical infrastructures, the life and physical integrity of people, damage to property and the environment, fundamental rights and the democratic process.

CHAPTER VIII
FROM THE PUBLIC HIGH-RISK ARTIFICIAL INTELLIGENCE DATABASE

Art. 44. The competent authority, in collaboration with the sectoral authorities, shall be responsible for creating and maintaining a publicly accessible high-risk AI database containing public documents on impact assessments, respecting commercial and industrial secrets, in accordance with the regulations and in compliance with the relevant legislation, in particular Law No. 13,709 of August 14, 2018 (General Personal Data Protection Law) and Law No. 12,527 of November 18, 2011 (Access to Information Law).

Sole paragraph. The creation of the central database does not prevent the creation of sectoral high-risk AI databases, which must be maintained in an interoperable format and with structured data to facilitate shared use.

CHAPTER IX
SUPERVISION AND INSPECTION

Section I
From the National System of Regulation and Governance of Artificial Intelligence

Art. 45. The Executive Branch is authorized to establish the National System of Regulation and Governance of Artificial Intelligence (SIA).

§ 1º The SIA comprises:

I – the National Data Protection Authority (ANPD), the competent authority that will coordinate the SIA;

II – sectoral authorities;

III – the Permanent Council for Regulatory Cooperation on Artificial Intelligence (Cria), observed and limited to the provisions of Section IV of this Chapter;

IV – the Committee of Experts and Scientists on Artificial Intelligence (Cecia), observed and limited to the provisions of Section V of this Chapter.

§ 2º An act of the federal Executive Branch will define a list of bodies and entities that will integrate the SIA, in accordance with items II, III and IV of § 1 of this article.

§ 3º The SIA has the following objectives and foundations:

I – enhance and reinforce the regulatory, sanctioning and normative powers of the sectoral authorities in harmony with the general related powers of the competent authority that coordinates the SIA; and

II – seek harmonization and collaboration with regulatory bodies on topics transversal.

§ 4º The competent authority will coordinate the Cria, as provided in Section IV. of this Chapter, in order to harmonize and facilitate regulatory, supervisory and sanctioning powers.

Art. 46. As coordinator of the SIA and without prejudice to the powers provided for in Law No. 13,709 of August 14, 2018 (General Law on the Protection of Personal Data), the competent authority is responsible for:

I – act as a representative of Brazil before international AI organizations, under the coordination of the Executive Branch;

II – issue, in collaboration with the other members of the SIA, binding rules of a general nature on the following topics:

a) form and requirements of the information to be published on the use of AI systems, respecting industrial and commercial secrets;

b) procedures and requirements for preparing the algorithmic impact assessment;

c) procedures for reporting serious incidents, particularly when they affect fundamental rights;

III – issue general rules on AI in the country, supporting sectoral bodies, which are responsible for issuing specific rules;

IV – enter into regulatory agreements with SIA members to define specific rules and procedures for coordinating competencies;

V – issue general normative guidelines on certificates and accreditation of certification bodies with the aim of encouraging and ensuring best governance practices throughout the entire life cycle of AI systems;

VI – encourage the adoption of internationally recognized standards, best practices and certifications;

VII – receive and process anonymous complaints, establishing confidentiality mechanisms identity of the whistleblower;

VIII – prepare annual reports on its activities.

Sole paragraph. In experimental regulatory environments (**sandboxes** regulatory) involving AI systems, conducted by sectoral authorities, the competent authority will be notified and may express its opinion on compliance with the purposes and principles of this Law.

Art. 47. As a residual regulator, the competent authority will exercise full normative, regulatory, supervisory and sanctioning powers for the development, implementation and use of AI systems for economic activities in which there is no specific sectoral regulatory body or entity.

Art. 48. The sectoral authority is responsible for:

I – exercise regulatory, supervisory and sanctioning powers, in accordance with its sphere of competence granted by law, for the development, implementation and use of AI systems;

II – issue specific rules for the application of AI, including aspects related to high-risk activities, in compliance with the general rules issued by the competent authority;

III – promote and encourage the provisions of Chapter VI of this Law for AI systems that fall within its sphere of competence granted by law;

IV – as regards its sphere of competence granted by law, encourage the adoption of internationally recognized standards, best practices and certification and accreditation models; V – supervise the

governance measures appropriate to each application or use of AI systems that it classifies as high risk, in order to promote:

a) harmonization with national legislation and international standards to allow technical and jurisdictional interoperability of systems and applications developed and implemented in the country;

b) the adoption of regulatory instruments that promote responsible innovation, such as experimental regulatory environments (**regulatory** sandboxes), self-regulation and certifications of good practices and governance;

VI – enter into, at any time, an agreement with AI 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.

(Law of Introduction to the Rules of Brazilian Law).

Section II

The Responsibilities and Powers of the Competent Authority

Art. 49. The competent authority shall:

I – ensure the protection of fundamental rights and other rights affected by use of AI systems;

II – promote and encourage the provisions of Chapter VI of this Law;

III – promote cooperation actions with protection authorities and promote the development and use of AI systems in other countries, of an international or transnational nature;

IV – request, at any time, from public authorities that develop or use AI systems, specific information on the scope and nature of the data and other details of the processing carried out, with the possibility of issuing a complementary technical opinion to ensure compliance with this Law;

V – enter into, together with the sectoral authorities, at any time, an agreement with AI agents to eliminate irregularities, legal uncertainty or contentious situations within the scope of administrative processes, in accordance with the provisions of Decree-Law No. 4,657, of September 4, 1942 (Law of Introduction to the Rules of Brazilian Law);

VI – prepare annual reports on its activities;

VII – carry out or determine audits of high-risk AI systems or those that produce relevant legal effects when necessary to assess compliance with this Law, ensuring confidential treatment of information, in light of commercial and industrial secrets;

VIII – accredit institutions, using criteria established in regulations subject to public consultation, for access to data for auditing and research purposes, ensuring the confidentiality of information, in compliance with commercial and industrial secrets;

IX – accredit research institutions, using criteria established in regulations subject to public consultation, for access to data for research purposes, observing commercial and industrial secrets, anonymization and protection of personal data, in accordance with Law No. 13,709, of August 14, 2018 (General Law on the Protection of Personal Data).

§ 1 Both the competent authority and any entities accredited by it to carry out audits and for research purposes must comply with information security and confidentiality requirements and personal data protection, in accordance with Law No. 13,709 of August 14, 2018 (General Personal Data Protection Law), with regard to commercial and industrial secrets.

§ 2^o The competent authority, together with the sectoral authorities, may carry out investigations into high-risk AI systems, in case of suspected violation of the principles, rights and duties provided for in this Law or in applicable sectoral legislation.

§ 3 The bodies and entities that are part of the SIA must immediately communicate to the Administrative Council for Economic Defense (CADE) any information identified during the course of inspection activities that may be of interest for the application of Law No. 12,529 of November 30, 2011 (Competition Defense Law).

§ 4^o In the exercise of its attributions and always within the limits of what is pertinent and necessary to determine concrete evidence of violations of the economic order, Cade may order developers to be granted access to training, validation and testing data sets used for the development of high-risk AI systems.

Section III Administrative Sanctions

Art. 50. AI agents, due to violations committed against the rules provided for in this Law, are subject to the following applicable administrative sanctions:

I – warning;

II – a simple fine, limited in total to R\$50,000,000.00 (fifty million reais) per violation, and in the case of a private legal entity, up to 2% (two percent) of its gross 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;

IV – prohibition or restriction on participating in the regulatory **sandbox** regime provided for in this Law, for up to 5 (five) years;

V – partial or total, temporary or permanent suspension of the development, supply or operation of the AI system;

VI – prohibition of processing certain databases.

§ 1^o The sanctions will be applied after an administrative procedure that allows the opportunity for a full defense, gradually, individually or cumulatively, according to the peculiarities of the specific case and considering the following parameters and criteria:

I – the severity and nature of the infractions and any violation of rights;

II – the good faith of the offender;

III – the advantage obtained or intended by the offender;

IV – the economic condition of the offender;

V – recidivism;

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 the analysis of algorithmic impact and the effective implementation of a code of ethics;

IX – the adoption of a good practices and governance policy;

X – the prompt adoption of corrective measures;

XI – the proportionality between the seriousness of the offence and the intensity of the sanction;

XII – cumulation with other administrative sanctions that may have already been definitively applied for the same unlawful act.

§ 2º Before or during the administrative process referred to in § 1º of this article, the competent authority may adopt preventive measures, including a punitive fine, observing the total limit referred to in item II of the **caput**, when there is evidence or well-founded fear that the AI agent:

I – causes or may cause irreparable or difficult to repair damage; or

II – render the final result of the process ineffective.

§ 3 The provisions of this article do not replace the application of administrative, civil or criminal sanctions defined in Law No. 8,078 of September 11, 1990 (Consumer Defense Code), in Law No. 13,709 of August 14, 2018 (General Law on the Protection of Personal Data), and in specific legislation.

§ 4 In the case of the development, supply or use of excessively risky AI systems, there will be, at a minimum, a fine and, in the case of a legal entity, partial or total, provisional or definitive suspension of its activities.

§ 5 The application of the sanctions provided for in this article does not exclude, under any circumstances, the obligation to fully repair the damage.

§ 6 The competent authority shall define, by means of its own regulation, the procedure for investigation and the criteria for applying administrative sanctions to violations of this Law, which shall be subject to:

I – public consultation and regulatory impact analysis, without prejudice to the provisions of Decree-Law No. 4,657 of September 4, 1942 (Law of Introduction to the Rules of Brazilian Law), Law No. 9,784 of January 29, 1999 (General Law of Administrative Procedure), and other pertinent legal provisions;

II – publication of methodologies that will objectively present the forms and dosages of sanctions, which must contain detailed justification for all their elements and demonstration of compliance with the criteria provided for in this Law.

§ 7º The provisions of items I, III, IV, V and VI of the **caput** of this article may be applied to public entities and bodies, without prejudice to the provisions of Law No. 8,112, of December 11, 1990 (Federal Public Servant Statute), in Law No. 8,429, of June 2

of 1992 (Law on Administrative Misconduct), and in Law No. 12,527 of November 18, 2011 (Access to Information Act).

Art. 51. The competent authority and sectoral authorities may carry out joint investigations into high-risk AI systems in cases of suspected violation of the principles, rights and duties provided for in this Law or in applicable sectoral legislation.

Art. 52. The bodies and entities that are part of the SIA must immediately communicate to the Administrative Council for Economic Defense (Cade) any information identified during the course of inspection activities that may be of potential interest for the application of Law No. 12,529 of November 30, 2011 (Competition Defense Law).

Sole paragraph. In the exercise of its powers and always within the limits of what is pertinent and necessary to determine concrete evidence of violations of the economic order, CADE may order developers to be granted access to training, validation and testing data sets used for the development of high-risk AI systems.

Section IV

From the Permanent Council for Regulatory Cooperation on Artificial Intelligence

Art. 53. The Permanent Council for Regulatory Cooperation on Artificial Intelligence (Cria) is hereby created, which will be responsible for producing guidelines and will be a permanent forum for collaboration, including through technical cooperation agreements, with sectoral authorities and civil society, in order to harmonize and facilitate the exercise of the powers of the competent authority.

Sole paragraph. It is the responsibility of the Cria:

- I – suggest actions to be carried out by the SIA;
- II – prepare studies and hold public debates on AI;
- III – disseminate knowledge about AI.

Section V

From the Committee of Experts and Scientists on Artificial Intelligence

Art. 54. The Committee of Experts and Scientists on Artificial Intelligence (Cecia) is hereby created with the aim of technically and scientifically guiding and supervising the development and application of AI in a responsible manner, under the terms defined by regulation.

CHAPTER X

FROM PROMOTING SUSTAINABLE INNOVATION

Section I

From the Experimental Regulatory Environment (Regulatory Sandbox)

Art. 55. The competent authority and the sectoral authorities that make up the SIA must promote and authorize the operation of an experimental regulatory environment for innovation in artificial intelligence (**AI regulatory sandbox**) on their own behalf or for entities that request it and meet the requirements specified by this Law and in regulations, including under a public-private cooperation regime.

§ 1 The regulatory **sandbox** aims to facilitate the development, testing and validation of innovative AI systems for a limited period before their placement on the market or putting into service in accordance with a specific plan, in order to develop innovative businesses in a safe manner.

§ 2 The competent authority and the sectoral authorities may, individually or in collaboration, within the scope of experimental regulatory environment programs (**regulatory sandbox**), exclude the incidence of standards under their jurisdiction in relation to the regulated entity or groups of regulated entities.

Art. 56. The competent authority and the sectoral authorities that make up the SIA will regulate the procedures for requesting and authorizing the operation of regulatory **sandboxes**, and may limit or interrupt their operation and issue recommendations, taking into account, among other aspects, the preservation of fundamental rights and the rights of potentially affected consumers, security and protection.

§ 1º Sectoral authorities must provide micro and small businesses, **startups** and public and private Scientific, Technological and Innovation Institutions (ICTs) with priority access to testing environments, as long as they comply with the eligibility conditions, selection criteria and other regulations.

§ 2º The competent authority and sectoral authorities may create mechanisms to reduce the regulatory costs of qualified entities in accordance with § 1º of the **caput** of this article.

Art. 57. Participants in the AI regulatory testing environment remain liable under applicable law for any damages inflicted on third parties as a result of experimentation taking place in the testing environment.

Section II

Guidelines for the protection of work and workers

Art. 58. The competent authority, the sectoral authorities that make up the SIA and the Permanent Council for Regulatory Cooperation on Artificial Intelligence (Cria), in cooperation with the Ministry of Labor, must develop guidelines for, among other objectives:

I – mitigate potential negative impacts on workers, especially those risks of job displacement and AI-related career opportunities;

II – enhance positive impacts on workers, especially to improve health and safety in the workplace;

- III – value the instruments of collective negotiations and agreements;
- IV – encourage the development of training programs and ongoing training for active workers, promoting professional development and improvement.

Section III **Incentive and Sustainability Measures**

Art. 59. Public administration within the Union, States, Federal District and Municipalities may promote innovation and productive and technological development in AI.

Sole paragraph. The development measures referred to in the **caput** will be guided by the following guidelines:

- I – promotion of innovation in the productive sectors, including through the contracting of innovative solutions by the State and the celebration of public-private partnerships under the terms of Law No. 11,079, of December 30, 2004;
- II – investment in research for the development of AI in the country, focused on the Brazilian socioeconomic context, valuing the country's technological and data autonomy and its insertion and competitiveness in the domestic and international markets;
- III – financing of hard-to-access AI physical and technological resources for small and medium-sized companies and research centers that promote sustainable practices;
- IV – encouraging the expansion of the availability of sustainable **data centers** with high data processing capacity for AI systems, with the densification of this production chain and related digital services in Brazil, with the aim of supporting the production sector and technical-scientific research and development;
- V – encouragement of the creation of multidisciplinary research and development centers and innovation in AI.

Art. 60. Public and private entities must prioritize the use of AI systems and applications that aim at energy efficiency and the rationalization of the consumption of natural resources.

Art. 61. Cria, in cooperation with the Ministry of Environment and Climate Change, will promote research and development of certification programs to reduce the environmental impact of AI systems.

Section IV **Copyright and Related Rights**

Art. 62. The AI developer who uses content protected by copyright and related rights must provide information about the protected content used in the development processes of AI systems, by publishing a summary on an easily accessible website, observing commercial and industrial secrets, in accordance with specific regulations.

Sole paragraph. For the purposes of this Chapter, development comprises the stages of mining, training, retraining, testing, validation and application of AI systems.

Art. 63. The automated use of protected content in text and data mining processes for the purposes of research and development of AI systems by scientific, research and educational organizations and institutions, museums, public archives and libraries does not constitute an offense to copyright and related rights, provided that the following conditions are met:

I – access was lawful;

II – not for commercial purposes;

III – the use of content protected by copyright and related rights is done to the extent necessary for the purpose to be achieved, without prejudice to the economic interests of the holders and without competition with the normal exploitation of the protected works and content.

§ 1 Copies of content protected by copyright and related rights used in AI systems must be stored in secure conditions, and only for the time necessary to carry out the activity or for the specific purpose of verifying the results.

§ 2^o The exhibition or dissemination of works and content protected by copyright is prohibited. copyright and related rights used in the development of AI systems.

§ 3 This article does not apply to institutions linked to, affiliated with or controlled by a for-profit entity that provides AI systems or that has, among them, a shareholding.

§ 4 The provisions of the **caput** of this article apply to data mining, by public or private entities, in the context of AI systems to combat civil and criminal offenses that violate copyright and related rights.

Art. 64. The holder of copyright and related rights may prohibit the use of content owned by him/her in the development of AI systems in cases not covered by art. 63 of this Law.

Sole paragraph. The prohibition of the use of protected works and content in the databases of an AI system after the training process does not exempt the AI agent from liability for moral and material losses and damages, under the applicable legislation.

Art. 65. The AI agent that uses content protected by copyright and related rights in mining, training or development processes of AI systems must remunerate the owners of such content due to such use, and must ensure:

I – that the holders of copyright and related rights have effective conditions to negotiate collectively, under the terms of Title VI of Law No. 9,610, of February 19, 1998 (Copyright Law), or directly the use of the contents of which they are holders, being able to do so free of charge or for a fee;

II – that the calculation of the remuneration referred to in the **caput** considers the principles of reasonableness and proportionality and relevant elements, such as the size of the AI agent and the competitive effects of the results in relation to the original content used;

III – free negotiation in the use of protected content, aiming to promote a research and experimentation environment that enables the development of innovative practices, and that does not restrict the freedom of agreement between the parties involved, under the terms of arts. 156, 157, 421, 422, 478 and 479 of Law No. 10,406, of January 10, 2002 (Civil Code), and art. 4 of Law No. 9,610, of February 19, 1998 (Copyright Law).

§ 1º The remuneration referred to in the **caput** of this article is only due:

I – to holders of national or foreign copyright and related rights domiciled in Brazil;

II – to persons domiciled in a country that ensures reciprocity in the protection, in terms equivalent to this article, of the copyright and related rights of Brazilians, as provided for in articles 2, sole paragraph, and 97, § 4, of Law No. 9,610, of February 19, 1998 (Copyright Law), with collection prohibited in cases where reciprocity is not assured.

§ 2º The holder of the right to remuneration provided for in the **caput** who opts for negotiation and direct authorization, under the terms of item I of the **caput**, may exercise it regardless of subsequent regulation.

Art. 66. The use of image, audio, voice or video content that portrays or identifies natural persons by AI systems must respect personality rights, as provided for in Law No. 10,406 of January 10, 2002 (Civil Code), and in relevant legislation.

Section V

From Incentive to Microenterprises, Small Businesses and Startups

Art. 67. Sectoral authorities must define differentiated criteria for AI systems offered by microenterprises, small businesses and **startups** that promote the development of the national technology industry.

Sole paragraph. Differentiated criteria must consider the competitive impact of related economic activities, the number of users affected and the nature of the economic activities carried out.

CHAPTER XI

ON THE ACTION OF THE PUBLIC AUTHORITIES

Section I

General Provisions

Art. 68. The following constitute guidelines for the actions of the Union, States, Federal District and Municipalities in the development of AI in Brazil:

I – establishment of mechanisms for multi-participatory, multi-sectoral, transparent, collaborative and democratic governance, with the participation of the government, the

business sector, third sector and academic community, especially considering vulnerable groups;

II – promoting trust in AI technologies, with the dissemination of information and knowledge about their ethical and responsible uses;

III – encouraging the training and preparation of people for the restructuring of the labor market;

IV – promoting interoperability between AI systems, including between different federative spheres and different sectors of society, with decisions that seek to avoid technological dependence and provide for the continued use of the systems developed or contracted;

V – advertising and dissemination of data, in an open, structured and secure manner;

VI – environmental protection and sustainable development;

VII – promoting international cooperation, by encouraging the sharing of knowledge about AI systems, in order to facilitate regulatory and technological interoperability;

VIII – promotion of investment in AI aimed at solving the country's problems, promoting its socioeconomic, cultural and environmental development, and for the development of the national and regional production system, valuing the country's technological autonomy and its insertion and competitiveness in the domestic and international markets.

Art. 69. AI systems of public authorities must seek to:

I – accessibility for people, regardless of their physical-motor, perceptive, sensory, intellectual, mental, cultural and social capabilities, safeguarding aspects of confidentiality and administrative and legal restrictions;

II – compatibility with both human reading and automated information processing;

III – ease of use of electronic government services that use systems
AI;

IV – ensuring transparency regarding the use of AI systems;

V – promotion of Portuguese culture and language;

VI – encouraging the development of national AI systems, with special attention to national issues and cultural, language and socioeconomic context nuances.

Section II Training, Qualification and Education

Art. 70. Public administration, within the scope of the Union, the States, the District Federal and Municipalities, will implement programs of:

I – education, training, qualification, and technical and higher education requalification in AI aligned with the demands of the market and the public sector;

II – digital literacy for meaningful, responsible and equitable use of available AI systems, prioritizing basic education;

III – support for workers impacted and possibly affected by the adoption of the AI, with a focus on promoting well-being, requalification, adaptation to new job market demands and professional reintegration;

IV – awareness and training in sustainability in the field of technologies advanced digital technologies, with an emphasis on responsible practices in the use of resources; and

V – encouraging educational institutions to include in their curricula subjects on environmental impact and sustainability in the development and operation of AI systems and applications and other advanced digital technologies.

§ 1º The programs referred to in the **caput** will seek to reduce inequalities, especially between the different regions of the country.

§ 2º The literacy measures referred to in item II of the **caput** will include basic notions and skills regarding AI systems and their operation, including the different types of products and uses, their risks and benefits.

Art. 71. The State must periodically formulate and promote studies, as well as establish goals, strategies, plans and schedules, regarding the use and development of AI in the Country.

CHAPTER XII

FINAL AND TRANSITORY PROVISIONS

Art. 72. The rights and principles expressed in this Law do not exclude others provided for in the national legal system or in international treaties to which the Federative Republic of Brazil is a party.

Art. 73. In order to promote national technological development, the SIA will regulate simplified regimes, involving flexibility of regulatory obligations provided for in this Law, in the following cases:

I – open and free standards and formats, with the exception of those considered to be of high risk or that fall within Section V of Chapter IV of this Law;

II – national promotion;

III – encouraging innovation and scientific and technological research in the production environment, with a view to technological training, achieving technological autonomy and developing the country's national and regional production system;

IV – projects of public interest and those that meet the priorities of industrial and science, technology and innovation policies and that are related to solving Brazilian problems;

V – projects carried out in public-private partnerships, or in strategic partnerships, in Scientific, Technological and Innovation Institutions (ICT), Technological Innovation Centers (NIT), support foundations, technology parks or technology hubs.

Sole paragraph. The Executive Branch shall provide for economic incentives in the cases provided for in the **caput** of this article.

Art. 74. In accordance with Chapter IX of this Law, the Executive Branch:

I – will provide, within 2 (two) years, the necessary resources to the ANPD, including for its administrative restructuring, in order to guarantee legal security and efficiency in the supervision and inspection of compliance with this Law;

II – will define the list of bodies and entities that will appear as sectoral authorities forming part of the SIA;

III – will define the detailed composition of the Cria;

IV – will define the role of the Administration’s Mediation and Conciliation Chamber Federal Public; and

V – will define the composition and powers of Cecia.

Art. 75. The **caput** of art. 3 of Law No. 14,533, of January 11, 2023 (Policy National Digital Education Code), shall come into force with the addition of the following section VI:

“Art. 3
.....

VI – critical algorithmic literacy and critical computing, which involves reading about the social and human implications of technologies, especially considering artificial intelligence.

....." (NR)

Art. 76. Art. 12 of Law No. 11,540, of November 12, 2007, shall come into force. added by the following § 6:

“Art. 12.
.....

§ 6º In the cases set out in item I of the **caput**, items “a”, “b” and “d”, priority will be given to the execution of artificial intelligence research and projects by various actors in the public and private sectors, or through public-private partnerships.” (NR)

Art. 77. The regulation of aspects associated with the circulation of **online** content and which may affect freedom of expression, including the use of AI for moderation and recommendation of content, may only be done through specific legislation.

Art. 78. The implementation of this Law will observe the perfect legal act, the law acquired and the res judicata.

Art. 79. Considering the impact of technological transformation, the SIA will be responsible, every four years, for promoting studies and issuing an opinion to be sent to the National Congress regarding the need to improve the standards established in this Law.

Art. 80. This Law shall come into force 730 (seven hundred and thirty) days after its official publication.

§ 1º The following shall come into force 180 (one hundred and eighty) days after the publication of this Law:

I – art. 13;

II – the rules set forth in Section V of Chapter IV; and

III – the rules set forth in Section IV of Chapter X, except for art. 62, which comes into effect immediately.

§ 2º The following shall come into force on the date of publication of this Law:

I – the provisions of Chapter IX, with the exception of art. 50;

II – the following Sections of Chapter X:

a) Section III; and

b) Section V.

Federal Senate, in of of .

Senator Rodrigo Pacheco
President of the Federal Senate