Bill of Law No. 2.338/23

CHAPTER I

PRELIMINARY PROVISIONS

Article 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 supervised systems, for the benefit of the individual human rights, the democratic regime, and the scientific and technological development.

Article 2. The development, implementation, and use of artificial intelligence systems in Brazil are based on:

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 self-determination;

IX – the promotion of research and development with the aim of stimulating innovation in the productive sectors and in the government;

X – access to information and education, as well as awareness of artificial intelligence systems and their applications.

Article 3. The development, implementation, and use of artificial intelligence systems shall 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;

VI – transparency, explainability, intelligibility, and auditability;

VII – reliability and robustness of artificial intelligence and information security systems;

VIII – due process of law, contestability, and adversary proceeding;

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, responsibility, and full compensation for damages;

XI – prevention, precaution, and mitigation of systemic risks derived from intentional or unintentional uses and unforeseen effects of artificial intelligence systems; and

XII – non-maleficence and proportionality between the methods employed and the determined and legitimate purposes of artificial intelligence systems.

Article 4. 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 forecasts, recommendations or decisions that may influence the virtual or real environment.

II – supplier of an artificial intelligence system: natural or legal person, whether governed by public or private law, who develops an artificial intelligence system, directly or on demand, 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;

III – operator of an artificial intelligence system: natural or legal person, whether governed by public or private law, who employs or uses, on their behalf or for their benefit, an artificial intelligence system, unless said system is used within the scope of a personal activity of unprofessional character.

IV – artificial intelligence agents: providers and operators of artificial intelligence systems.

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, whose 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.

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 and legitimate justification in light of the right to equality and other fundamental rights;

VIII – text and data mining: process of extraction and analysis of large amounts of data or partial or full excerpts of textual content, from which patterns and correlations are extracted, which will generate relevant information for the development or use of artificial intelligence systems.

CHAPTER II

RIGHTS

Section I - General Provisions

Article 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:

I – right to prior information regarding their interactions with artificial intelligence systems;

II – right to an explanation about the decision, recommendation or forecast made by artificial intelligence systems;

III – right to challenge decisions or forecasts of artificial intelligence systems that produce legal effects or that significantly impact the interests of the affected party;

IV – right to determination and human participation in decisions on artificial intelligence systems, considering the context and the state of the art of technological development;

V – right to non-discrimination and correction of direct, indirect, illegal, or abusive discriminatory biases; and

VI – right to privacy and protection of personal data, under the terms of the relevant legislation.

Sole Paragraph. The artificial intelligence agents shall inform, in a clear and easily accessible way, the necessary procedures for the exercise of the rights described in the head of this article.

Article 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.

Section II - Rights Associated with Information and Understanding of Decisions Made by Artificial Intelligence Systems

Article 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:

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 forecasts intended to be made 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 operation of the artificial intelligence system;

VI – security, non-discrimination, and reliability measures adopted, including accuracy, precision, and coverage; and

VII – other information defined by regulation.

§1 Without prejudice to the provision of complete information in a physical or digital media open to the public, the information referred to in item I of the head provision of this article shall also be provided, when appropriate, with the use of easily recognizable icons or symbols.

§2 Persons exposed to emotion recognition systems or biometric categorization systems shall be informed about the use and operation of the system in the environment where exposure occurs.

§3 The artificial intelligence systems that are intended for vulnerable groups, such as children, adolescents, the elderly, and people with disabilities, shall be developed in such a way that these people are able to understand how they work and their rights vis-à-vis artificial intelligence agents.

Article 8. The person affected by the artificial intelligence system may request an explanation of the decision, forecast or recommendation, with information regarding the criteria and procedures used, as well as the main factors that affect such specific forecast or decision, including information on:

I – the rationality and logic of the system, as well as the meaning and expected consequences of such a decision for the affected person;

II – the degree and level of contribution of the artificial intelligence system to decision-making;

III – the data processed and their source, as well as the decision-making criteria and, where appropriate, their weighting, applied to the situation of the affected person;

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 head provision shall be provided by a free and facilitated procedure, in a language that allows the person to understand the result of the decision or forecast in question, within a period of up to fifteen days from the request, with the possibility of extension, once, for an equal period, depending on the complexity of the case.

Section III - The Right to Challenge Decisions and Request Human Intervention

Article 9. The person affected by an artificial intelligence system shall have the right to contest and request the review of decisions, recommendations or forecasts generated by such system that produce relevant legal effects or that significantly impact their interests.

§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 data or data processed in violation

of the legislation, under the terms of art. 18 of Law No. 13,709, of August 14, 2018 and the relevant legislation.

§2 The right to challenge provided for in the head provision of this article also covers decisions, recommendations or forecasts supported by discriminatory, unreasonable inferences or others that violate objective good faith, thus understood the inferences that:

I – are based on inadequate or abusive data for the purposes of the processing;

II – are based on imprecise or statistically unreliable methods; or

III – do not adequately consider the individuality and personal characteristics of individuals.

Article 10. When the decision, forecast or recommendation of an artificial intelligence system produces relevant legal effects or effects that significantly impact the interests of the person, including through the generation of profiles and the making of inferences, the person may request human intervention or review.

Sole Paragraph. Human intervention or review shall not be required if its implementation proves to be impossible, in which case the person responsible for operating the artificial intelligence system shall implement effective alternative measures to ensure the reanalysis of the contested decision, considering the arguments raised by the affected person, as well as repair any damage caused.

Article 11. In scenarios in which decisions, forecasts 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.

Section IV - The Right to Non-Discrimination and Correction of Direct, Indirect, Illegal or Abusive Discriminatory Biases

Article 12. People affected by decisions, forecasts 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:

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

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 head provision does not prevent the adoption of differentiation criteria between individuals or groups when such differentiation is based on demonstrated, reasonable, and legitimate objectives or justifications considering the right to equality and other fundamental rights.

CHAPTER III

RISK CATEGORIZATION

Section I - Preliminary Assessment

Article 13. Before being placed on the market or used in service, every artificial intelligence system shall undergo a preliminary assessment carried out by the supplier to classify its degree of risk, whose registration shall consider the criteria provided for in this chapter.

§1 The suppliers of general-purpose artificial intelligence systems shall include in their preliminary assessment the purposes or applications indicated, pursuant to article 17 of this law.

§2 There will be a record and documentation of the preliminary assessment carried out by the supplier for responsibility and accountability purposes if the artificial intelligence system is not classified as high risk.

§3 The competent authority may determine the reclassification of the artificial intelligence system, upon prior notification, as well as determine the performance of an algorithmic impact assessment for the instruction of the ongoing investigation.

§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 shall be mandatory, without prejudice to any penalties in the event of a fraudulent, incomplete or untrue preliminary assessment.

Section II - Excessive Risk

Article 14. The implementation and use of artificial intelligence systems are prohibited:

I – when they 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;

II – when they 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;

III – by the government, when they assess, 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 way.

Article 15. Within the scope of public security activities, the continuous use of remote biometric identification systems is only permitted in spaces accessible to the public, when provided for in a 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 prison sentence of more than two years;

II – search for victims of crimes or missing people;

III – crime in flagrante delicto.

Sole Paragraph. The law referred to in the head provision shall provide for proportionate and strictly necessary measures to serve the public interest, subject to due process of law and judicial control, as well as the principles and rights provided for in this Law, especially the guarantee against discrimination and the need for review of the algorithmic inference by the public official in charge before taking any action against the identified person.

Article 16. The competent authority shall be responsible for regulating excessively risky artificial intelligence systems.

Section III – High Risk

Article 17. High-risk artificial intelligence systems are those used for the following purposes:

I – application as safety devices in the management and operation of critical infrastructures, such as traffic control and water and electricity supply networks;

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;

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;

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 cases 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, to identify unknown patterns or discover hidden relationships in the data;

XIII – investigation by administrative authorities to assess the credibility of evidence during investigation or repression of infringements, to forecast 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.

Article 18. Tthe competent authority shall be responsible for updating the list of excessive or high-risk artificial intelligence systems, identifying new hypotheses, based on at least one of the following criteria:

I - the implementation is on a large scale, considering the number of people affected and the geographic extent, as well as its duration and frequency;

II - the system may negatively impact the exercise of rights and freedoms or the use of a service;

III - the system has a high potential for pecuniary and moral damage, in addition to being discriminatory;

IV - the system affects people from a specific vulnerable group;

V - the possible harmful results of the artificial intelligence system are irreversible or difficult to reverse;

VI - a similar artificial intelligence system has previously caused pecuniary or moral damage;

VII - low degree of transparency, explainability, and auditability of the artificial intelligence system, which makes its control or supervision difficult;

VIII - 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;

IX - 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 shall be preceded by consultation with the competent sectoral regulatory body, if any, as well as public consultation and hearings and analysis of the regulatory impact.

CHAPTER IV

GOVERNANCE OF ARTIFICIAL INTELLIGENCE SYSTEMS

Section I – General Provisions

Article 19. Artificial intelligence agents shall 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:

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 from conception 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.

§1 The governance measures of artificial intelligence systems are applicable throughout their life cycle, from the initial conception to the closure of their activities and discontinuation.

§2 The technical documentation of high-risk artificial intelligence systems shall 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.

Section II - Governance Measures for High-Risk Artificial Intelligence Systems

Article 20. In addition to the measures indicated in article 19, artificial intelligence agents providing or operating high-risk systems shall 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;

II – use of tools for automat recording of the system's operation, in order to allow the assessment of its accuracy and robustness and determine discriminatory potentials, as well as the implementation of adopted risk mitigation measures, with special attention to adverse effects;

III – testing 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;

b) composition of an inclusive team responsible for the design and development of the system, guided by the pursuit of diversity.

V – adoption of technical measures to enable the explanation of the results of artificial intelligence systems and 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 shall use their best efforts 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, allowing 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 excessively rely on the result produced by the artificial intelligence system;

III – correctly interpret the result of the artificial intelligence system, considering the characteristics of the system and the tools and methods of interpretation available;

IV – decide, in any specific situation, not to use the high-risk artificial intelligence system or ignore, annul, or reverse its result;

V – intervene in the operation of the high-risk artificial intelligence system or interrupt its operation.

Article 21. In addition to the governance measures established in this chapter, bodies and entities of the Union, States, Federal District, and Municipalities, when contracting, developing or using artificial intelligence systems considered to be of high risk, shall adopt the following measures:

I – hold 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;

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 party, 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 provisions of article 43.

§1 The use of biometric systems by the government of the Union, States, Federal District, and Municipalities shall 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.

§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 shall be discontinued.

Section III - Algorithmic Impact Assessment

Article 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.

Sole Paragraph. The competent authority shall be notified of the high-risk system by sharing preliminary and algorithmic impact assessments.

Article 23. The algorithmic impact assessment shall 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.

Sole Paragraph. The competent authority shall be responsible for regulating 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;

Article 24. The impact assessment methodology shall contain, at least, the following steps:

I – preparation;

II – risk cognition;

III – mitigation of the risks found;

IV – monitoring.

§1 The impact assessment shall 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;

b) benefits associated with the artificial intelligence system;

c) likelihood of adverse consequences, including the number of people potentially impacted;

d) severity of adverse consequences, including the effort required to mitigate them;

e) operating logic of the artificial intelligence system;

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);

§2 Following 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 consider incipient, incomplete, or speculative evidence.

§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.

§4 The competent authority shall be responsible for regulating the periodicity of update of impact assessments, considering the life cycle of high-risk artificial intelligence systems and the fields of application, and best sectoral practices may be incorporated.

§5 The artificial intelligence agents who, after their 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.

Article 25. The algorithmic impact assessment shall consist of a continuous iterative process, performed throughout the entire lifecycle of high-risk artificial intelligence systems, requiring periodic updates.

§1 The competent authority shall be responsible for regulating the periodicity of update of impact assessments.

§2 The update of the algorithmic impact assessment shall also have public participation, based on a stakeholder consultation procedure, albeit in a simplified manner.

Article 26. Industrial and commercial secrets being guaranteed, the conclusions of the impact assessment shall be public, containing at least the following information:

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 any, under the terms of § 3 of article 24 of this Law.

CHAPTER V

CIVIL LIABILITY

Article 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.

§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.

§2 When it is not a high-risk artificial intelligence system, the guilt of the agent causing the damage shall be presumed, applying the reversal of the burden of proof in favor of the victim.

Article 28. Artificial intelligence agents shall not be liable when they:

I – prove that they have not put into circulation, used, or taken advantage of the artificial intelligence system; or

II – prove that the damage is due exclusively to the victim or a third party, as well as an external fortuitous event.

Article 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. 8,078, of September 11, 1990 (Consumer Protection Code), without prejudice to the application other provisions of this Law.

CHAPTER VI

CODES OF GOOD PRACTICES AND GOVERNANCE

Article 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.

§1 When establishing rules of good practices, the purpose, probability, and severity of the risks and resulting benefits shall be considered, following the example of the methodology set forth in article 24 of this law;

§ 2 The developers and operators of artificial intelligence systems may:

I – implement a governance program that, at least:

a) demonstrates its commitment to adopting internal processes and policies that ensure comprehensive compliance with rules and good practices related to 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 article 24, § 3, of this Law;

d) is integrated into its overall governance structure and establishes and applies internal and external oversight mechanisms;

e) has 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;

§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 considered by the competent authority for the purpose of applying administrative sanctions.

§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

REPORT OF SERIOUS INCIDENTS

Article 31. Artificial intelligence agents shall 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.

§1 The communication shall be made within a reasonable time, as defined by the competent authority.

§2 The competent authority shall 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

IMPLEMENTATION AND SUPERVISION

Section I - Competent Authority

Article 32. The Executive Branch shall designate the competent authority to ensure the implementation and supervision of this Law.

Sole Paragraph. The competent authority is responsible for:

I – ensuring the protection of fundamental rights and other rights affected by the use of artificial intelligence systems;

II – promoting the elaboration, updating, and implementation of the Brazilian Artificial Intelligence Strategy with the bodies of related competence;

III – promoting and preparing studies on good practices in the development and use of artificial intelligence systems;

IV – encouraging the adoption of good practices, including codes of conduct, in the development and use of artificial intelligence systems;

V – promoting 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;

VI – issuing rules for the regulation of this Law, including on:

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;

d) procedures for certifying the development and use of high-risk systems.

VII – articulating with public regulatory authorities to exercise their competences in specific sectors of economic and governmental activities subject to regulation;

VIII – inspecting, independently or jointly with other competent public bodies, the disclosure of information provided for in articles 7 and 43;

IX – inspecting and applying sanctions in the event of development or use of artificial intelligence systems carried out in breach of legislation, through administrative proceedings that ensure adversary proceeding, fair hearing, and the right of appeal;

X – requesting, at any time, from 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 – assuming, 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 – considering 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 the regulation;

XIII – preparing annual reports on its activities.

Sole Paragraph. When exercising the attributions of the head provision, the competent body may establish conditions, requirements, communication channels, and differentiated disclosure for suppliers and operators of artificial intelligence systems qualified as small or very small companies, under the terms of Complementary Law No. 123, of December 14, 2006, and startups, pursuant to Complementary Law No. 182, of June 1st, 2021.

Article 33. The competent authority shall be the central body for the application of this Law and the establishment of norms and guidelines for its implementation.

Article 34. The competent authority and the bodies and public entities responsible for regulating specific sectors of economic and governmental activity shall coordinate their activities, in the corresponding spheres of action, with a view to ensuring compliance with this Law.

§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, to facilitate their regulatory, inspection, and sanctioning powers.

§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 shall be informed, being able to express its opinion regarding the fulfillment of the purposes and principles of this law.

Article 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 articles 6 to 12 of Law No. 13,848, of June 25, 2019, where applicable.

Section II - Administrative Sanctions

Article 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 fifty million reais (BRL 50,000,000.00) per infraction, being, in the case of a legal entity governed by private law, up to two percent (2%) 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;

IV – prohibition or restriction to participate in the regulatory sandbox regime provided for in this law, for up to five years;

V – partial or total suspension, temporary or definitive, of the development, supply, or operation of the artificial intelligence system; and

VI – prohibition of processing of certain databases.

§1 The sanctions shall be applied after an administrative procedure that allows the opportunity for fair hearing, 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;

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

X – prompt adoption of corrective measures;

XI – 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.

§2 Before or during the administrative process of § 1, the competent authority may adopt preventive measures, including a fine, subject to the total limit referred to in item II of the head provision, 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 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, Law No. 13,709, of August 14, 2018, and in specific legislation.

§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.

§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 article 27.

Article 37. The competent authority shall 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 September 4, 1942, Law No. 9,784 of January 29, 1999, and other relevant legal provisions.

Sole Paragraph. The methodologies referred to in the head provision of this article shall be published in advance and shall objectively present the forms and dosimetry of the sanctions, which will contain detailed grounds for all their elements, demonstrating compliance with the criteria provided for in this Law.

Section III – Measures to Foster Innovation

Article 38. The competent authority may authorize the operation 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.

Article 39. Authorization requests for regulatory sandboxes shall be submitted to the competent body through a project whose characteristics include, among others:

I - innovation in the use of technology or in the alternative use of existing technologies;

II - improvements in terms of efficiency gains, cost reduction, increased safety, risk reduction, benefits to society and consumers, among others;

III - discontinuity plan, with forecast of measures to be taken to ensure the operational viability of the project once the regulatory sandbox authorization period has ended.

Article 40. The competent authority shall 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, considering, 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.

Article 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 to third parties as a result of the experimentation that takes place in the testing environment.

Article 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, 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 holders' economic interests;

IV – it does not compete with the normal exploitation of the works.

§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.

§2 The provisions of the head provision apply to data and text mining activities for other analytical activities in artificial intelligence systems, subject to the conditions set out in the head provision and paragraph 1, provided that the activities do not communicate the work to the public and that access to the works is given legitimately.

§3 The text and data mining activity involving personal data shall be subject to the provisions of Law No. 13,709, of August 14, 2018 (General Data Protection Law).

Section III - Artificial intelligence public database

Article 43. The competent authority is responsible for creating and maintaining 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.

CHAPTER IX

FINAL PROVISIONS

Article 44. 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.

Article 45. This law comes into force one year after its publication.