BILL NO. , OF 2023

Provides for the use of Artificial Intelligence.

THE NATIONAL CONGRESS decrees:

CHAPTER I
PRELIMINARY PROVISIONS

Art. 1 This Law establishes general rules of a national nature for the development, implementation and responsible use of artificial intelligence (AI) systems in Brazil, with the aim of protecting fundamental rights and ensuring the implementation of safe and reliable systems, for the benefit of the human person, the democratic regime and scientific and technological development.

Art. 2 The development, implementation and use of systems of artificial intelligence 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 personality;

IV – environmental protection and development sustainable;

V – equality, non-discrimination, plurality and respect to labor rights;

VI – technological development and innovation;

VII – free initiative, free competition and the defense of consumer;

VIII – privacy, data protection and self-determination informative;

IX – the promotion of research and development with the purpose of stimulating innovation in the productive sectors and in the public sector; and

X – access to information and education, and awareness about artificial intelligence systems and their applications.

Art. 3 The development, implementation and use of systems of artificial intelligence will observe good faith and the following principles:

I – inclusive growth, sustainable development and well-being be;

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 intelligence systems artificial and information security;

VIII – due process, contestability and adversarial system;

IX – traceability of decisions throughout the life cycle of artificial intelligence systems as a means of accountability and assignment of responsibilities to a natural or legal person;

X – accountability, responsibility and full reparation of damages;

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

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

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

I – artificial intelligence system: computer system, with different degrees of autonomy, designed to infer how to achieve a given set of objectives, using approaches based on machine learning and/or logic and knowledge representation, through input data from machines or humans, with the aim of producing predictions, recommendations or decisions that can influence the virtual or real environment;

II – artificial intelligence system provider: natural person or legal entity, whether public or private, that develops an artificial intelligence 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;

III – artificial intelligence system operator: natural person or legal entity, whether public or private, that employs or uses, in its name or benefit, an artificial intelligence system, unless said system is used within the scope of a personal activity of a non-professional nature;

IV – artificial intelligence agents: suppliers and operators of artificial intelligence systems;

V – competent authority: body or entity of the Administration Federal Public Authority responsible for overseeing, implementing and monitoring compliance with this Law throughout the national territory;

VI – 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 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 geographical origin, race, color or ethnicity, gender, sexual orientation, socioeconomic class, age, disability, religion or political opinions;

VII – indirect discrimination: discrimination that occurs when apparently neutral normative, practical or criterion has the capacity to disadvantage people belonging to a specific group, or place them at a disadvantage, unless such regulation, practice or criterion has some reasonable and legitimate objective or justification in light of the right to equality and other fundamental rights;

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

CHAPTER II
OF RIGHTS

Section I
General Provisions

Art. 5 People affected by artificial intelligence systems have the following rights, to be exercised in the manner and under the conditions described in this Chapter:

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 predictions of systems artificial intelligence that produces legal effects or that significantly impacts the interests of the affected party;

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

V – right to non-discrimination and correction of biases directly, indirectly, illegally or abusively discriminatory; and

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

Sole paragraph. Artificial intelligence agents will inform, in a clear and easily accessible manner, the procedures necessary for exercising the rights described in*caput*.

Art. 6 The defense of the interests and rights provided for in this Law may be exercised before the competent administrative bodies, as well as in court, individually or collectively, in accordance with the provisions of the relevant legislation regarding individual, collective and diffuse protection instruments.

Section II
Rights associated with information and understanding of decisions taken by artificial intelligence systems

Art. 7 People affected by artificial intelligence systems have the right to receive, prior to contracting or using the system, clear and adequate information regarding the following aspects:

I – automated nature of interaction and decision making in processes or products that affect the person;

II – general description of the system, types of decisions, recommendations or predictions it is intended to make and the consequences of its use for the person;

III – identification of intelligence system operators artificial and governance measures adopted in the development and use of the system by the organization;

IV – role of artificial intelligence system and humans involved in the decision-making, forecasting or recommendation process;

V – categories of personal data used in the context of operation of the artificial intelligence system;

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

VII – other information defined in regulations.

§ 1º Without prejudice to the provision of information in a manner complete in physical or digital media open to the public, the information referred to in item I of*caput*of this article will also be provided, where appropriate, with the use of easily recognizable icons or symbols.

§ 2º People exposed to emotion recognition systems or biometric categorization systems will be informed about the use and operation of the system in the environment in which the exposure occurs.

§ 3 Artificial intelligence systems intended for groups vulnerable people, such as children, adolescents, the elderly and people with disabilities, will be developed in such a way that these people can understand how they work and their rights in the face of artificial intelligence agents.

Art. 8 The person affected by artificial intelligence system You may request an explanation of the decision, forecast or recommendation, with information about the criteria and procedures used, as well as the main factors affecting such specific forecast or decision, including information about:

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

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

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

IV – the mechanisms through which the person can contest the decision; and

V – the possibility of requesting human intervention, under the terms of this Law.

Sole paragraph. The information mentioned in the*caput*will be provided through a free and facilitated procedure, in 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 an extension once, for the same period, depending on the complexity of the case.

Section III
The right to contest decisions and request human intervention

Art. 9 The person affected by the artificial intelligence system will have the right to contest and request review of decisions, recommendations or predictions generated by such system that produce relevant legal effects or that significantly impact your interests.

§ 1º The right to correct incomplete data is guaranteed, inaccurate or outdated used by artificial intelligence systems, as well as the right to request the anonymization, blocking or deletion of unnecessary, excessive data or data processed in non-compliance with the legislation, in accordance with art. 18 of Law No. 13,709, of August 14, 2018 and the relevant legislation.

§ 2º The right to contest provided for in*caput*this article covers also decisions, recommendations or forecasts supported by discriminatory, unreasonable inferences or those that violate objective good faith, thus understood as inferences that:

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

II – are based on imprecise or statistically inaccurate methods not reliable; or

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

Art. 10. When the system decision, prediction or recommendation If artificial intelligence produces relevant legal effects or significantly impacts the interests of the person, including through the generation of profiles and the making of inferences, the person may request human intervention or review.

Sole paragraph. Human intervention or review will not be required if its implementation is demonstrably impossible, in which case the person responsible for operating the artificial intelligence system will implement effective alternative measures in order to ensure the reanalysis of the contested decision, taking into account the arguments raised by the affected person, as well as the compensation for any damages caused.

Art. 11. In scenarios where decisions, predictions or recommendations generated by artificial intelligence systems have an irreversible or difficult to reverse impact or involve decisions that may generate risks to the life or physical integrity of individuals, there will be significant human involvement in the decision-making process and final human determination.

Section IV
The right to non-discrimination and the correction of direct discriminatory biases, indirect, illegal or abusive

Art. 12. People affected by decisions, predictions or recommendations of artificial intelligence systems are entitled to treatment fair and equitable, 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 – based on the establishment of disadvantages or worsening of the vulnerability of people belonging to a specific group, even when apparently neutral criteria are used.

Sole paragraph. The sealing provided for in the*caput*does not prevent the adoption of criteria for differentiating between individuals or groups when such differentiation occurs based on demonstrated, reasonable and legitimate objectives or justifications in light of the right to equality and other fundamental rights.

CHAPTER III
RISK CATEGORIZATION

Section I
Preliminary assessment

Art. 13. Prior to its placement on the market or use in service, every artificial intelligence system will undergo a preliminary assessment carried out by the supplier to classify its degree of risk, the registration of which will consider the criteria set out in this chapter.

§ 1º Suppliers of artificial intelligence systems general purpose will include in their preliminary assessment the purposes or applications indicated, in accordance with art. 17 of this law.

§ 2º There will be a record and documentation of the preliminary assessment. carried out by the supplier for accountability and accountability purposes in the event that 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 to instruct the ongoing investigation.

§ 4 If the result of the reclassification identifies the system of artificial intelligence as high risk, the performance of an algorithmic impact assessment and the adoption of other governance measures provided for in Chapter IV will be mandatory, without prejudice to any penalties in the event of a fraudulent, incomplete or false preliminary assessment.

Section II
Excessive Risk

Art. 14. The implementation and use of systems of artificial intelligence:

I – that employ subliminal techniques that aim to or inducing a natural person to behave in a manner that is harmful or dangerous to their health or safety or against the foundations of this Law;

II – that exploit any group vulnerabilities specific to 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 public authorities, to evaluate, classify or rank the 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.

Art. 15. Within the scope of public security activities, it is only the use of remote biometric identification systems is permitted, continuously in spaces accessible to the public, when provided for in specific federal law and judicial authorization in connection with the activity of individualized criminal prosecution, in the following cases:

I – prosecution of crimes punishable by a maximum penalty of imprisonment more than two years;

II – search for victims of crimes or missing persons; or

III – crime in flagrante.

Sole paragraph. The law referred to in the*caput*will provide measures proportional and strictly necessary to meet the public interest, observing due process 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 algorithmic inference by the agent responsible public, before taking any action against the identified person.

Art. 16. It will be up to the competent authority to regulate the systems of excessive risk artificial intelligence.

Section III
High Risk

Art. 17. Artificial intelligence systems are considered high risk those used for the following purposes:

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

II – education and vocational training, including training systems determining access to educational or vocational training institutions or for the assessment and monitoring of students;

III – recruitment, screening, filtering, evaluation of candidates, making decisions on promotions or terminations of employment contracts, assignment of tasks and monitoring and evaluation of the performance and behavior of persons affected by such applications of artificial intelligence in the areas of employment, management of workers and access to self-employment;

IV – assessment of access, eligibility and concession criteria, 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 – assessment of people’s debt capacity natural or establishing your credit rating;

VI – sending or establishing priorities for services emergency response, including fire 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 generate risks to physical integrity of people;

IX – applications in the health area, including those intended to assist medical diagnoses and procedures;

X – biometric identification systems;

XI – criminal investigation and public safety, especially for individual risk assessments by competent authorities in order to determine the risk of a person committing or reoffending offences, or the risk to potential victims of criminal offences or to assess the personality traits and characteristics or past criminal behaviour of individuals or groups;

XII – analytical study of crimes relating to natural persons, enabling law enforcement authorities to search large, complex, related or unrelated data sets available from different data sources or in different data formats, in order to identify unknown patterns or discover hidden relationships in the data;

XIII – investigation by administrative authorities to assess the credibility of evidence in the course of 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; or

XIV – migration management and border control.

Art. 18. It will be up to the competent authority to update the list of excessive or high-risk artificial intelligence systems, identifying new hypotheses, based on at least one of the following criteria:

I – the implementation is on a large scale, taking into account consideration of the number of people affected and the geographical extent, as well as their 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 material or moral as well as discriminatory;

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

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

VI – a similar artificial intelligence system has caused previously material or moral damages;

VII – low degree of transparency, explainability and auditability of the artificial intelligence system, which makes it difficult to control or supervise;

VIII – high level of identifiability of data subjects, including the processing of genetic and biometric data for the purposes of uniquely identifying a natural person, in particular where the processing involves combining, matching or comparing data from multiple sources;

IX – when there are reasonable expectations of the affected party regarding the use of your personal data in the artificial intelligence system, in particular the expectation of confidentiality, such as in the processing of confidential or sensitive data.

Sole paragraph. The update of the list mentioned in*caput*for the competent authority will be preceded by consultation with the competent sectoral regulatory body, if any, as well as by public consultation and hearing and regulatory impact analysis.

CHAPTER IV
ON THE GOVERNANCE OF ARTIFICIAL INTELLIGENCE SYSTEMS

Section I
General Provisions

Art. 19. Artificial intelligence agents will establish governance structures and internal processes capable of guaranteeing the security of systems and the fulfillment of the rights of affected persons, 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 systems artificial intelligence in interaction with natural persons, which includes the use of appropriate and sufficiently clear and informative human-machine interfaces;

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 for mitigation and prevention of potential discriminatory biases;

IV – legitimacy of data processing in accordance with the legislation of data protection, including through the adoption of privacy measures by design and by default and the adoption of techniques that minimize the use of personal data;

V – adoption of appropriate separation and organization parameters data for training, testing and validating system results; and

VI – adoption of appropriate information security measures from design to system operation.

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

§ 2º Technical documentation of artificial intelligence systems high-risk information will be prepared before it is made available on the market or used to provide services and will be kept up to date during its use.

Section II
Governance Measures for High-Risk Artificial Intelligence Systems

Art. 20. In addition to the measures indicated in art. 19, the agents of artificial intelligence that provide or operate high-risk systems will adopt the following governance measures and internal processes:

I – documentation, in the format appropriate to the process development and technology used, regarding the functioning of the system and the decisions involved in its construction, implementation and use, considering all relevant stages in the system life cycle, such as the development stage*design*, development, evaluation, operation and discontinuation of the system;

II – use of automatic operation recording tools system, in order to allow the assessment of its accuracy and robustness and to determine potential discrimination, and implementation of the risk mitigation measures adopted, with special attention to adverse effects;

III – carrying out tests to assess appropriate levels of reliability, depending on the sector and type of application of the artificial intelligence system, including robustness, accuracy, precision and coverage tests;

IV – data management measures to mitigate and prevent bias discriminatory, including:

a) evaluation of data with appropriate control measures human cognitive biases that may affect data collection and organization and to avoid the generation of biases due to problems in classification, failures or lack of information regarding affected groups, lack of coverage or distortions in representation, depending on the intended application, as well as corrective measures to avoid the incorporation of structural social biases that may be perpetuated and amplified by technology; and

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

V – adoption of technical measures to enable explainability 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 relevant criteria for producing results, as well as, upon request by the interested party, providing adequate information that allows the interpretation of the results actually produced, respecting industrial and commercial confidentiality.

Sole paragraph. Human supervision of intelligence systems High-risk artificial intelligence shall seek to prevent or minimize risks to the rights and freedoms of individuals that may arise from its normal use or from its use under reasonably foreseeable conditions of misuse, enabling those responsible for human supervision to:

I – understand the capabilities and limitations of the system artificial intelligence 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 trust automatically or rely excessively on the result produced by the artificial intelligence system;

III – correctly interpret the result of the system artificial intelligence taking into account the characteristics of the system and the available tools and interpretation methods;

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

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

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

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

III – use of data from secure 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 power public, the right to human explanation and review of decisions made 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 application programming interface that allow its use by other systems for interoperability purposes, in accordance with regulations; and

VI – publication in easily accessible vehicles, preferably on their websites, of preliminary assessments of 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 art. 43.

§ 1º The use of biometric systems by public authorities Union, States, Federal District and Municipalities will be preceded by the publication 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 data on race, color or ethnicity is prohibited, unless expressly provided for by law.

§ 2º If elimination or substantive mitigation is not possible of the risks associated with the artificial intelligence system identified in the algorithmic impact assessment provided for in Article 22 of this Law, its use will be discontinued.

Section III
Algorithmic Impact Assessment

Art. 22. Algorithmic impact assessment of information systems artificial intelligence is the obligation of artificial intelligence agents, whenever the system is considered high risk by the preliminary assessment.

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

Art. 23. The algorithmic impact assessment will be carried out by professional or team of professionals with the technical, scientific and legal knowledge necessary to prepare the report and with functional independence.

Sole paragraph. It will be up to the competent authority to regulate the cases in which the performance or audit of the impact assessment will necessarily be conducted by a professional or team of professionals external to the supplier;

Art. 24. The impact assessment methodology will contain, at least the following steps:

I – preparation;

II – risk cognition;

III – mitigation of risks found;

IV – monitoring.

§ 1º The impact assessment will consider and record, at least:

a) known and foreseeable risks associated with the system artificial intelligence 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 potentially impacted people;

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

e) operating logic of the artificial intelligence system;

f) process and results of tests and evaluations and measures of mitigation carried out to verify possible impacts on rights, with special emphasis on potential discriminatory impacts;

g) training and awareness-raising actions on the risks associated with artificial intelligence system;

h) mitigation measures and indication and justification of risk residual of the artificial intelligence system, accompanied by frequent quality control tests; and

i) transparency measures to the public, especially to potential users of the system, regarding residual risks, especially when involving a high degree of harm or danger to the health or safety of users, in accordance with articles 9 and 10 of Law No. 8,078, of September 11, 1990 (Consumer Defense Code).

§ 2º In compliance with the precautionary principle, when using of artificial intelligence systems that may generate irreversible or difficult-to-reverse impacts, the algorithmic impact assessment will also take into account incipient, incomplete or speculative evidence.

§ 3 The competent authority may establish other criteria and elements for preparing an impact assessment, including the participation of the different social segments affected, according to the risk and economic size of the organization.

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

§ 5º Artificial intelligence agents that, after their introduction into the market or use in service, have knowledge of unexpected risk that they present to the rights of natural persons, will immediately communicate the fact to the competent authorities and to the people affected by the artificial intelligence system.

Art. 25. The algorithmic impact assessment will consist of continuous iterative process, executed throughout the entire life cycle of high-risk artificial intelligence systems, requiring periodic updates.

§ 1º The competent authority shall be responsible for regulating the frequency of updating impact assessments.

§ 2º The update of the algorithmic impact assessment will count also with public participation, based on a consultation procedure with interested parties, albeit in a simplified manner.

Art. 26. Industrial and commercial secrets are 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 level residual, once such measures have been implemented; and

III – description of the participation of different affected segments, if it has occurred, in accordance with § 3 of art. 24 of this Law.

CHAPTER V
CIVIL LIABILITY

Art. 27. The intelligence system provider or operator artificial damage that causes patrimonial, moral, individual or collective damage is obliged to repair it in full, regardless of the degree of autonomy of the system.

§ 1º When dealing with a high-level artificial intelligence system, risk or excessive risk, the supplier or operator is objectively liable for the damages caused, to the extent of their participation in the damage.

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

Art. 28. Artificial intelligence agents will not be held accountable when:

I – prove that they did not put into circulation, employ or took advantage of the artificial intelligence system; or

II – prove that the damage is due to a fact exclusive to the victim or third party, as well as external fortuitous events.

Art. 29. The hypotheses of civil liability arising from damages caused by artificial intelligence systems in the context of consumer relations remain subject to the rules set forth in Law No. 8,078 of September 11, 1990 (Consumer Defense Code), without prejudice to the application of the other rules of this Law.

CHAPTER VI
CODES OF GOOD PRACTICE AND GOVERNANCE

Art. 30. Artificial intelligence agents will be able to, individually or through associations, formulate codes of good practice and governance that establish the organizational conditions, operating regime, procedures, including those regarding complaints from affected parties, safety standards, technical standards, specific obligations for each implementation context, educational actions, internal mechanisms for supervision and risk mitigation and appropriate technical and organizational security measures for managing risks arising from the application of the systems.

§ 1º When establishing rules of good practice, they will be considering the purpose, probability and severity of the risks and resulting benefits, following the example of the methodology set out in art. 24 of this Law.

§ 2º Developers and operators of intelligence systems artificial, may:

I – implement a governance program that, at a minimum:

a) demonstrate your commitment to adopting processes and internal policies that ensure comprehensive compliance with standards and good practices relating 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 their harmful potential;

c) has the objective of establishing a relationship of trust with the affected people, through transparent action that ensures participation mechanisms in accordance with art. 24, § 3, of this Law;

d) is integrated into its overall governance structure and establishes and apply internal and external supervision mechanisms;

e) have response plans to reverse possible harmful results of the artificial intelligence system; and

f) is constantly updated based on information obtained from continuous monitoring and periodic assessments.

§ 3 Voluntary adherence to a code of good practices and governance may be considered indicative of good faith on the part of the agent and will be taken into account by the competent authority for the purposes of applying administrative sanctions.

§ 4º The competent authority may establish a procedure for analysis of the compatibility of the code of conduct with current legislation, with a view to its approval, publication and periodic updating.

CHAPTER VII
ON THE REPORTING OF SERIOUS INCIDENTS

Art. 31. Artificial intelligence agents will communicate 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 the functioning of critical infrastructure operations, serious damage to property or the environment, as well as serious violations of fundamental rights, in accordance with the regulation.

§ 1º The communication will be made within a reasonable period, as per defined by the competent authority.

§ 2º The competent 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.

CHAPTER VIII
SUPERVISION AND INSPECTION

Section I
From the Competent Authority

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

Sole paragraph. It is up to the competent authority to:

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

II – promote the preparation, updating and implementation of Brazilian Artificial Intelligence Strategy with related competent bodies;

III – promote and prepare studies on good practices in development and use of artificial intelligence systems;

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

V – promote cooperation actions with protection authorities and to promote the development and use of artificial intelligence systems from other countries, whether international or transnational in nature;

VI – issue 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 assessment of algorithmic impact;

c) form and requirements of the information to be published about the use of artificial intelligence systems; and

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

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

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

IX – monitor and apply sanctions, in case of development or use of artificial intelligence systems carried out in breach of legislation, through an administrative process that ensures adversarial proceedings, full defense and the right to appeal;

X – request, at any time, from public authorities that develop or use artificial intelligence systems, specific information 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 ensure compliance with this Law;

XI – enter into, at any time, an agreement with agents of artificial intelligence to eliminate irregularities, legal uncertainty or contentious situations in administrative proceedings, in accordance with the provisions of Decree-Law No. 4,657 of September 4, 1942;

XII – assess petitions against the system operator artificial intelligence, after proven presentation of a complaint not resolved within the period established in the regulations; and

XIII – prepare annual reports on its activities.

Sole paragraph. When exercising the powers of the*caput*, the organ The competent authority may establish conditions, requirements, communication and dissemination channels differentiated for suppliers and operators of artificial intelligence systems qualified as micro or small companies, under the terms of Complementary Law No. 123, of December 14, 2006, and*startups*, under the terms of Complementary Law No. 182, of June 1, 2021.

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

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

§ 1º The competent authority shall maintain a permanent forum for communication, including through technical cooperation, with public administration bodies and entities responsible for regulating specific sectors of economic and governmental activity, in order to facilitate their regulatory, supervisory and sanctioning powers.

§ 2º In experimental regulatory environments (*sandbox* regulatory) involving artificial intelligence systems, conducted by public bodies and entities responsible for regulating specific sectors of economic activity, the competent authority will be notified and may express its opinion on compliance with the purposes and principles of this law.

Art. 35. The regulations and standards issued by the authority competent authority will be preceded by public consultation and hearing, as well as regulatory impact analyses, in accordance with articles 6 to 12 of Law No. 13,848, of June 25, 2019, where applicable.

Section II
Administrative Sanctions

Art. 36. Artificial intelligence agents, due to the Violations committed against the rules provided for in this Law are subject to the following administrative sanctions applicable by the competent authority:

I – warning;

II – simple fine, limited in total to R$50,000,000.00 (fifty million reais) per violation, being, in the case of a private law legal entity, up to 2% (two percent) of its turnover, of its group or conglomerate in Brazil in its last fiscal year, excluding taxes;

III – publication of the infraction after it has been duly investigated and confirmed its occurrence;

IV – prohibition or restriction to participate in a regime*sandbox* regulatory framework provided for in this Law, for up to five years;

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

VI – prohibition of processing certain databases.

§ 1º The sanctions will be applied after administrative proceedings. that allows the opportunity for a broad defense, gradually, isolated or cumulatively, according to the peculiarities of the specific case and considering the following parameters and criteria:

I – the gravity and nature of the infractions and the possible 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 mechanisms and internal procedures capable of minimizing risks, including algorithmic impact analysis and 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 fault and the intensity of the sanction; and

XII – cumulation with other administrative sanctions eventually already applied definitively for the same unlawful act.

§ 2 Before or during the administrative process of § 1, the competent authority to adopt preventive measures, including a punitive fine, observing the total limit referred to in item II of*caput*, when there is evidence or well-founded fear that the artificial intelligence 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 sanctions administrative, civil or criminal as defined in Law No. 8,078 of September 11, 1990, in Law No. 13,709 of August 14, 2018, and in specific legislation.

§ 4 In the case of the development, supply or use of excessive risk artificial intelligence systems will, at the very least, result in a fine being applied 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, in in any event, the obligation to fully repair the damage caused, under the terms of art. 27.

Art. 37. The competent authority shall define, by means of own regulation, the procedure for determining and criteria for applying administrative sanctions to 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*caput*of this article will be published in advance and will objectively present the forms and dosage of the sanctions, which will contain detailed justification for all their elements, demonstrating compliance with the criteria provided for in this Law.

Section III
Measures to foster innovation

Art. 38. The competent authority may authorize the operation of an experimental regulatory environment for innovation in artificial intelligence (*sandbox*regulatory) for entities that request it and meet the requirements specified by this Law and in regulations.

Art. 39. Requests for authorization to*sandboxes* regulatory measures will be presented 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 towards efficiency gains, reduction costs, increased security, reduced risks, benefits to society and consumers, among others;

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

Art. 40. The competent authority shall issue regulations for establish procedures for requesting and authorizing the operation of *sandboxes*regulatory, being able to limit or interrupt its operation, as well as issue recommendations, taking into account, among other aspects, the preservation of fundamental rights, the rights of potentially affected consumers and the security and protection of personal data that are subject to processing.

Art. 41. Participants in the testing environment regulation of artificial intelligence continue to be liable, under applicable liability legislation, for any damages inflicted on third parties as a result of experimentation taking place in the testing environment.

Art. 42. The use of this does not constitute copyright infringement. automated processing of works, such as extraction, reproduction, storage and transformation, in data and text mining processes in artificial intelligence systems, in activities carried out by research and journalism organizations and institutions and by museums, archives and libraries, provided that:

I – do not have as their objective the simple reproduction, exhibition or dissemination of the original work itself;

II – use occurs to the extent necessary for the purpose to be achieved. achieved;

III – does not unjustifiably harm the interests economic rights of the holders; and

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

§ 1º Any reproductions of works for mining activities data 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 scientific research.

§ 2º The provisions of the following apply:*caput*to the mining activity of data and texts for other analytical activities in artificial intelligence systems, provided that the conditions of the items of the*caput*and § 1, provided that the activities do not communicate the work to the public and that access to the works has been legitimate.

§ 3º Text and data mining activity involving data personal data will be subject to the provisions of Law No. 13,709, of August 14, 2018 (General Law on the Protection of Personal Data).

Section IV
Public Artificial Intelligence Database

Art. 43. It is up to the competent authority to create and maintain a publicly accessible high-risk artificial intelligence database containing public impact assessment documents, respecting commercial and industrial secrets, in accordance with the regulation.

CHAPTER IX
FINAL PROVISIONS

Art. 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.

Art. 45. This Law shall come into force one year after its publication.

JUSTIFICATION

The development and popularization of technologies Artificial intelligence has revolutionized several areas of human activity. Furthermore, predictions indicate that artificial intelligence (AI) will bring about even more profound economic and social changes in the near future.

Recognizing the relevance of this issue, some propositions legislative proposals have recently been presented, both in the Federal Senate and in the Chamber of Deputies, with the aim of establishing guidelines for the development and application of artificial intelligence systems in Brazil. In particular, Bill (PL) No. 5,051, of 2019, authored by Senator Styvenson Valentim, stands out, which*establishes the principles for the use of Artificial Intelligence in Brazil*; Bill No. 21, 2020, by Federal Deputy Eduardo Bismarck, which*establishes foundations, principles and guidelines for the development and application of artificial intelligence in Brazil; and provides other measures*, and which was approved by the Chamber of Deputies; and PL No. 872, of 2021, by Senator Veneziano Vital do Rêgo, which*provides for the use of Artificial Intelligence*.

On February 3, 2022, these three projects began to be processed jointly in the Federal Senate and, subsequently, on February 17 of the same year, through the Act of the President of the Federal Senate No. 4, of 2022, of my authorship, at the suggestion of Senator Eduardo Gomes, with the aim of preparing a legal text with the most advanced technicality, the Committee of Jurists was established to support the preparation of a draft of a substitute for them.

Composed of renowned jurists, the commission had as members great experts in the fields of civil law and digital law, to whom I would like to thank for their time, dedication and sharing of the final text, which I now present. The following members of the collegiate body were: the Minister of the Superior Court of Justice, Ricardo Villas Bôas Cueva (President); Laura Schertel Ferreira Mendes (Rapporteur); Ana de Oliveira Frazão; Bruno Ricardo Bioni; Danilo Cesar Maganhoto Doneda (*in memoriam*); I would also like to thank the technical staff of the Federal Senate, especially the Legislative Consultancy and the civil servants who provided support to the collegiate: Reinilson Prado dos Santos; Renata Felix Perez and Donaldo Portela Rodrigues.

The said Commission held a series of public hearings, in addition to an international seminar, where more than seventy experts on the subject were heard, representing various segments: organized civil society, government, academia and the private sector. It also opened up the opportunity for any interested parties to participate, through written contributions, having received 102 statements, individually analyzed and organized according to their proposals. Finally, the Committee requested the Legislative Consultancy of the Federal Senate to study the regulation of artificial intelligence in more than thirty member countries of the Organization for Economic Cooperation and Development (OECD), which allowed for an analysis of the global regulatory panorama on the subject.

Based on all this extensive material, on December 6, 2022, the Commission of Jurists presented its final report, along with a draft bill for the regulation of artificial intelligence.

In this context, this initiative is based on the conclusions of the mentioned Commission and seeks to reconcile, in legal discipline, the protection of rights and fundamental freedoms, the appreciation of work and human dignity and technological innovation represented by artificial intelligence.

The project has a dual objective. On the one hand, it establishes rights to protect the most vulnerable link in question, the natural person who is already impacted daily by artificial intelligence systems, from content recommendation and advertising targeting on the Internet to their eligibility analysis for taking out credit and for certain public policies. On the other hand, by having governance tools and an institutional arrangement for monitoring and supervision, it creates conditions for predictability regarding its interpretation and, ultimately, legal certainty for innovation and technological development.

The proposition is based on the premise, therefore, that there is no*trade-off*between the protection of fundamental rights and freedoms, the valorization of work and the dignity of the human person in the face of the economic order and the creation of new value chains. On the contrary, its foundations and its principled basis seek such harmonization, in accordance with the Federal Constitution.

Structurally, the proposal establishes a regulation based on in risks and a regulatory model based on rights. It also presents governance instruments for adequate accountability of economic agents that develop and use artificial intelligence, encouraging good faith action and effective risk management.

The proposed text initially defines foundations and principles general provisions for the development and use of artificial intelligence systems, which guide all other specific provisions.

Dedicates a specific chapter to the protection of people's rights affected by artificial intelligence systems, which: ensures appropriate access to information and adequate understanding of the decisions taken by these systems; establishes and regulates the right to contest automated decisions and to request human intervention; and regulates the right to non-discrimination and the correction of discriminatory biases.

In addition to establishing basic and transversal rights for each and every one context in which there is interaction between machine and human being, such as information and transparency, this obligation is intensified when the AI system produces relevant legal effects or impacts subjects in a significant way (e.g.: right to contest and human intervention). Thus, the weight of regulation is calibrated according to the potential risks of the context in which the technology is applied. Certain rights were established in a symmetrical manner general and specific governance measures for, respectively, artificial intelligence systems with any degree of risk and for those categorized as high risk.

When addressing the categorization of artificial intelligence risks, the The proposal establishes the requirement for preliminary assessment; defines prohibited applications due to excessive risk; and defines high-risk applications, subject to stricter control standards.

Regarding systems governance, the project lists the measures to be adopted to ensure transparency and mitigation of biases; sets additional measures for high-risk systems and for government artificial intelligence systems; and standardizes the procedure for algorithmic impact assessment.

The text also addresses the rules of civil liability involving artificial intelligence systems, including defining the cases in which those responsible for their development and use will not be held liable.

According to the gradation of standards according to the risk imposed by the system - which permeates the entire draft of the proposal - an important distinction is made in the chapter on civil liability: when it concerns a high-risk or excessive-risk AI system, the supplier or operator is objectively liable for the damages caused, to the extent of each one's participation in the damage. And when it concerns AI that is not high-risk, the fault of the agent causing the damage will be presumed, applying the reversal of the burden of proof in favor of the victim.

The project also strengthens protection against discrimination, by through various instruments, such as the right to information and understanding, the right to contest, and a specific right to correct direct, indirect, illegal or abusive discriminatory biases, in addition to preventive governance measures. In addition to adopting definitions on direct and indirect discrimination – thus incorporating definitions from the Inter-American Convention against Racism, enacted in 2022 –, the text focuses on (hyper)vulnerable groups both for the qualification of what may be a high-risk system and for the reinforcement of certain rights.

When providing for the monitoring of artificial intelligence, the project determines that the Executive Branch designates an authority to ensure compliance with the established standards and specifies its powers and establishes administrative sanctions.

Measures are also planned to foster innovation in artificial intelligence, highlighting the experimental regulatory environment (*sandbox*regulatory).

With this, from a mixed approach of provisions*ex-ante* and*ex post*, the proposal outlines criteria for the purposes of evaluating and triggering which types of actions should be taken to mitigate the risks at stake, also involving the sectors interested in the regulatory process, through co-regulation.

Furthermore, in line with international law, it sets out guidelines for to conform copyright and intellectual property rights to the notion that data should be a common good and, therefore, circulate for machine training and the development of artificial intelligence systems - without, however, implying harm to the holders of such rights. This has implications for how regulation can foster innovation. In view of the above, and aware of the challenge that the matter represents, we count on the collaboration of our distinguished colleagues to improve this proposal.

Session Room,

Senator Rodrigo Pacheco