CESCON
BARRIEU

AI LEGAL FRAMEWORK

KEY ASPECTS OF THE TEXT APPROVED BY THE SENATE

BILL NO. 2.338/23

On December 10, 2024, the Federal Senate approved **Bill No. 2,338/2023 (“Bill”), known as the Artificial Intelligence Legal Framework**. The Bill aims to establish general guidelines for the responsible governance of Artificial Intelligence (“AI”) systems in Brazil, structured around fundamental principles such as human-centricity, privacy and personal data protection, transparency, and auditability. Strongly inspired by the EU AI Act, the Bill adopts a risk-based classification system for AI systems according to their respective risk level. The key provisions of the approved text are outlined below.

SCOPE

The rules of the Bill apply to all operations involving the development, deployment, and use of AI Systems, defined as “machine-based systems that, with varying degrees of autonomy and for explicit or implicit purposes, infer, from a set of data or information received, how to generate outputs, in particular predictions, content, recommendations, or decisions that may influence the virtual, physical, or real environment”.

The Bill also distinguishes between different categories of AI Systems, such as **general-purpose AI** and **generative AI**, establishing specific obligations for the development, deployment, and use of each of them.

AI AGENTS

The AI value chain comprises various agents. In general terms, the Bill organizes them into **three main groups**, assigning to each of them specific responsibilities and governance obligations.

DISTRIBUTOR

A natural or legal person, whether public or private, that makes an AI system available and distributes it for use by a third party, either for a fee or free of charge.

DEVELOPER

A natural or legal person, whether public or private, that develops an AI System, directly or by commission, with the purpose of placing it on the market or applying it in a service they provide.

USER

A natural or legal person, whether public or private, that employs or uses an AI System on their behalf or for their benefit.

RIGHTS

Individuals or groups affected by AI Systems have the following rights:

ALL AI SYSTEMS

Right to information regarding interactions with AI Systems;

Right to privacy and personal data protection;

Right to protection against unlawful or abusive discrimination and to the correction of illegal or abusive discriminatory biases.

HIGH-RISK AI SYSTEMS

Right to an explanation regarding the decision, recommendation, or prediction made by the AI System;

Right to contest and request a review of decisions, recommendations, or predictions made by the AI System;

Right to human review of decisions.

GENERATIVE AI SYSTEMS

Transparency regarding the copyright or related rights used in the development of AI Systems;

Right to compensation for the use of copyright or related rights;

Right to opt-out from the use of copyright or related rights in the development of AI Systems.

RISK CLASSIFICATION

The Bill adopts a risk-based approach, classifying AI Systems according to their potential impact level. **It sets specific requirements for high-risk systems and prohibits the use of systems deemed as "excessive risk".**

EXCESSIVE RISK

AI Systems implemented to (i) instigate, induce, or exploit vulnerabilities with the purpose of inducing behaviors that cause harm to health, safety, or other fundamental rights; (ii) assess personality traits, characteristics, or past behaviors for the purpose of evaluating the risk of committing crimes, offenses, or recidivism; (iii) classify or rank individuals based on social behavior or personality attributes; (iv) enable the production, dissemination, or facilitate the creation of material that constitutes or represents the abuse or exploitation of children and adolescents. As these are risks that cannot be tolerated, given their potential for harm to fundamental rights, the development, deployment, and use of such AI Systems are prohibited.

HIGH RISK

AI Systems implemented for use as security devices in managing critical infrastructure, education, recruitment, screening, filtering and evaluation of candidates, decision-making regarding promotions or terminations of employment relationships, assessing access criteria, reducing or revoking essential services (including public welfare and social security services), autonomous vehicles in public spaces, and applications in the health sector. These may be used, provided that appropriate risk management measures are observed.

GOVERNANCE

ALL CHAIN AGENTS

GENERAL OBLIGATIONS

- Ensure system safety and the rights of those affected
- Cooperate and provide information to the authority
- Include an identifier in generated synthetic content
- Report the occurrence of a serious incident to the authority

HIGH-RISK SYSTEMS

- Inform procedures for the exercise of data subjects' rights
- Report unexpected risks or impacts to the authority and other chain agents

DEVELOPERS

GENERAL OBLIGATIONS

- Prevent the system from being used for prohibited purposes
- Publish a summary of protected content used in development
- Compensate intellectual property rights holders for content used in training

GENERAL-PURPOSE AI / GENERATIVE AI SYSTEMS:

- Conduct a preliminary risk assessment
- Document the model, tests, risks, and datasets
- Prepare technical documentation and usage instructions
- Design systems in a sustainable manner
- Cooperate in risk mitigation

HIGH-RISK SYSTEMS

- Maintain a record of governance measures
- Log system operation
- Conduct security testing
- Provide information to interpret generated outputs
- Mitigate and prevent discriminatory biases
- Share assessments with the sectoral authority
- **Conduct an Algorithmic Impact Assessment (AIA)**

DEPLOYERS

HIGH-RISK SYSTEMS

- Document all stages of the system’s lifecycle
- Evaluate the results of system use
- Document reliability and security testing
- Document the degree of human oversight effectively maintained
- Provide information to interpret results
- Mitigate and prevent discriminatory biases
- **Conduct an Algorithmic Impact Assessment (AIA)**

DISTRIBUTORS

HIGH-RISK SYSTEMS

- Support and verify compliance with governance measures by other chain agents

ALGORITHMIC IMPACT ASSESSMENT (AIA)

Obligation required of Developers and Deployers. The AIA must identify, analyze, and mitigate algorithmic risks, with attention to: biases that may distort diagnoses; automated decisions affecting the data subject's health; and impacts on vulnerable groups. Developers must share the assessments with the competent sectoral authority.

ENFORCEMENT

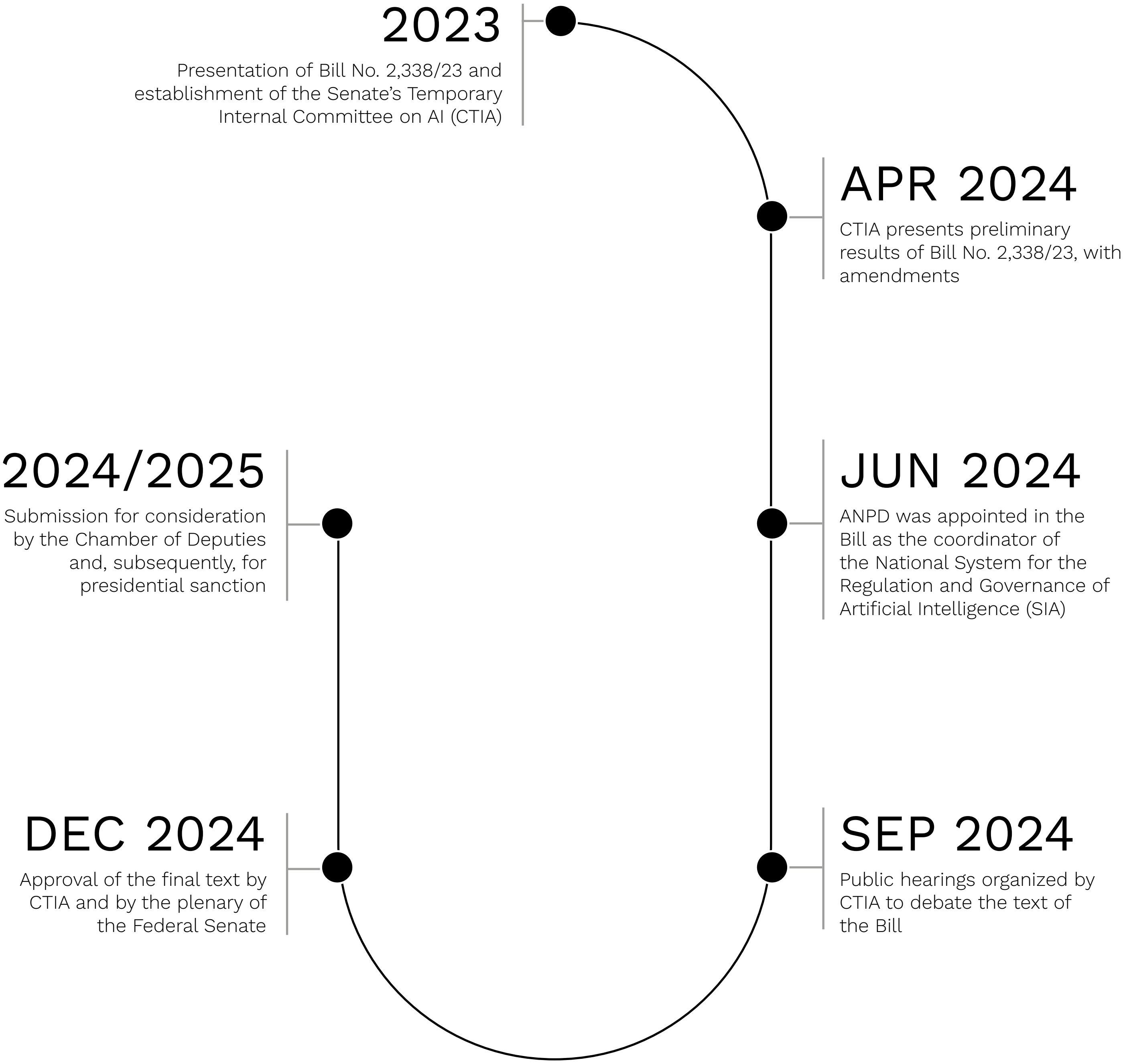
The Bill established the **National System for the Regulation and Governance of Artificial Intelligence ("SIA")**, a regulatory ecosystem that, according to the current text, will be coordinated by the **National Data Protection Agency ("ANPD")**.

The ANPD and the sectoral authorities within the SIA have oversight and enforcement powers. In the event of non-compliance with the AI Legal Framework, they may impose one or more sanctioning measures, as listed:

SANCTIONS

- Warning
- Simple fine (limited to 50 million BRL or 2% of gross revenue)
- Public disclosure of the infraction
- Prohibition or restriction from participating in the AI sandbox regime (for up to 5 years)
- Partial or total suspension of the development, provision, or operation of the AI system
- Prohibition on processing certain data sets

LEGISLATIVE PROCESS AND NEXT STEPS



2023

Presentation of Bill No. 2,338/23 and establishment of the Senate's Temporary Internal Committee on AI (CTIA)

APR 2024

CTIA presents preliminary results of Bill No. 2,338/23, with amendments

JUN 2024

ANPD was appointed in the Bill as the coordinator of the National System for the Regulation and Governance of Artificial Intelligence (SIA)

SEP 2024

Public hearings organized by CTIA to debate the text of the Bill

DEC 2024

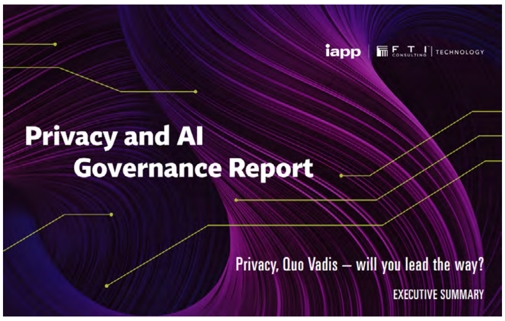
Approval of the final text by CTIA and by the plenary of the Federal Senate

2024/2025

Submission for consideration by the Chamber of Deputies and, subsequently, for presidential sanction

A PATH OF NO RETURN

Considering the imminent AI Legal Framework, it is essential for organizations to begin structuring an **AI governance program**. The goal is to foster innovation without compromising the legal certainty of the organization, its employees, or third parties. Any action taken at this stage will significantly reduce the effort required to implement an AI governance program in the near future.



iapp | FTI CONSULTING | TECHNOLOGY

Privacy and AI Governance Report

Privacy, Quo Vadis – will you lead the way?

EXECUTIVE SUMMARY

The Privacy and AI Governance Report, published by the International Association of Privacy Professionals (IAPP), shows that organizations are already directing efforts toward this structuring. In fact, 50% of the organizations surveyed indicated that they are building AI governance based on existing privacy and personal data protection governance practices.

WHERE TO START?

AI is a cross-functional and multidisciplinary topic, requiring not only legal expertise but also technical knowledge from teams such as information technology, information security, product development, and data governance. In this context, it may be beneficial to begin AI governance by establishing an AI and ethics committee, bringing together professionals from different backgrounds to ensure an integrated and holistic perspective. From this committee, additional actions may include:

APPROVED TOOLS

It is essential that the IT team conducts a thorough analysis and formally approves AI tools, technically assessing their reliability from an information security perspective.

CLEAR POLICIES

The legal department, in collaboration with other teams such as IT and information security, should develop specific and clear policies on the use of AI within the organization. These policies should cover aspects such as restrictions on the use of approved tools, guidelines for the proper use of the technology, data anonymization requirements, and other essential measures to ensure compliance, security, and ethical use of AI.

VENDOR MANAGEMENT

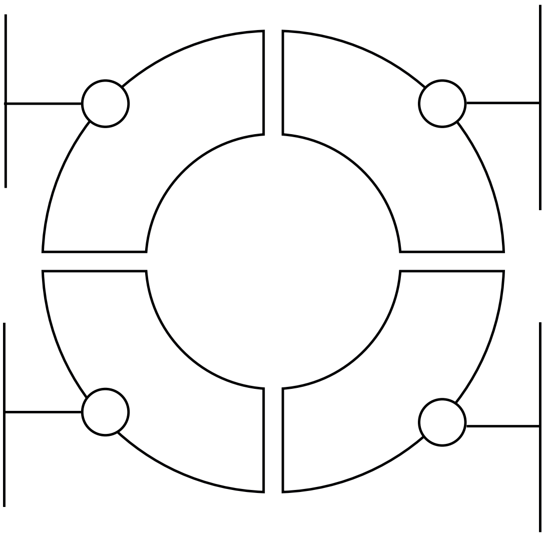
The organization may already use AI vendors or contract services supported by this technology. In this context, it is essential to review the organization's standard contractual clauses, ensuring they include AI-specific provisions whenever necessary, in order to guarantee compliance, security, and alignment with ethical practices.

TRAINING AND AWARENESS

The legal department should promote training sessions and awareness initiatives focused on the lawful and ethical use of AI tools. To enhance the effectiveness of these initiatives, it is advisable to consider engaging subject-matter experts. These trainings represent an excellent opportunity to reinforce internal policies and the organization's position on the topic, aligning employees with corporate guidelines and values.

HOW CAN WE HELP?

Cescon Barrieu is a full-service law firm with a highly specialized team in Law and Technology. Our work on AI governance projects is primarily based on the **AI Risk Management Framework (AI RMF)**, developed by the National Institute of Standards and Technology (NIST), a widely recognized model that guides the identification, assessment, and mitigation of risks related to AI. **This framework is structured around the following pillars:**



METRICS

Metrics, parameters, and processes for measuring the program and the risks related to the development and/or use of AI.

MAPPING

Understanding the context of AI use or development within the organization. Strategies and the creation of processes that enable the organization to identify AI use cases and risks.

GOVERNANCE

Policies and instruments related to the mapping, measurement, and management of AI risks. Awareness initiatives and the allocation of responsibilities to address the topic.

MANAGEMENT

Processes and instruments related to managing the risks identified and assessed by the organization. Strategies, processes, and clauses to address risks related to third-party contracting.

Based on our expertise and the AI RMF, we have developed a range of services specifically designed to address the ethical and legal challenges associated with AI. This approach allows us to offer, in addition to legal advisory on structuring AI governance programs, comprehensive support and execution in any legal matter related to the topic, including:

- REVIEW AND NEGOTIATION OF CONTRACTS INVOLVING AI
- TRAINING AND AWARENESS INITIATIVES ON THE USE OF AI
- POLICIES, GUIDELINES, AND OTHER DOCUMENTS RELATED TO AI GOVERNANCE
- ASSESSMENT OF LEGAL RISKS IN AI-RELATED VENDOR CONTRACTING
- RISK ASSESSMENT AND ALGORITHMIC IMPACT EVALUATION
- MAPPING AND RISK ANALYSIS OF AI SYSTEMS USED BY THE COMPANY

Cescon Barrieu has a highly specialized technology team with extensive experience in strategic transactions and advisory in the areas of artificial intelligence, data protection, intellectual property, and other disciplines related to innovation. Our team is composed of lawyers recognized in the market, led by partners and professionals with deep expertise in technology.

If you have any legal questions related to AI governance, please do not hesitate to contact one of our partners:

CONTACT US

JOYCE HONDA

PARTNER | ANTITRUST

joyce.honda@cesconbarrieu.com.br

JULIA PAZOS

PARTNER | TECHNOLOGY AND INNOVATION

julia.pazos@cesconbarrieu.com.br

LIOR PINSKY

PARTNER | M&A

lior.pinsky@cesconbarrieu.com.br

TANIA LIBERMAN

PARTNER | TECHNOLOGY AND INNOVATION

tania.liberman@cesconbarrieu.com.br

THAYS GENTIL

PARTNER | TECHNOLOGY AND INNOVATION

thays.gentil@cesconbarrieu.com.br