AI Governance in Corporations: Legal Frontiers and the Brazilian Experience

Artificial Intelligence is not just a tool. It is a new actor in corporate decision-making – and that demands legal accountability. This presentation explores the evolving landscape of AI governance in Brazil, offering insights for corporate leaders, legal professionals, and policymakers navigating this complex intersection of technology and law.

About the Speaker

Professional Background

- Licensed attorney in Brazil, Germany, and Portugal
- Specialization in Digital Law, Data Protection, and Artificial Intelligence
- Legal expert to the Brazilian Congress
- Advisor to the National Council of Justice (CNJ)
- Member of the Brazilian Bar Institute (IAB)
- DPO of the Brazilian Bar
- Certified Chief AI Officer
- LLM, PhD Candidate

With over a decade of experience at the intersection of technology and law, I have advised multinational corporations, governmental bodies, and judicial institutions on the implementation of legally compliant AI systems. My work focuses on creating frameworks that balance innovation with accountability and human rights protection.

In today's presentation, I will share insights from Brazil's pioneering approach to AI regulation, examining how corporations can prepare for the evolving legal landscape while leveraging AI for enhanced governance and compliance.

The Brazilian AI Regulatory Landscape

1

Senate Bill No. 2.338/2023

Brazil's primary legislative initiative governing artificial intelligence, drawing significant inspiration from the European Union's AI Act. The bill establishes a comprehensive framework for AI development, deployment, and governance across all sectors of the Brazilian economy.

- Currently advancing through legislative committees
- Expected implementation timeline: 2024-2025
- Strong cross-party support for core provisions

2

Risk-Based Regulatory Approach

Following global best practices, Brazil has adopted a tiered approach to AI regulation based on potential harm:

- **Unacceptable Risk:** Systems that pose threats to fundamental rights (prohibited)
- **High Risk:** Applications in critical sectors requiring rigorous oversight
- **Minimal Risk:** Systems with limited potential for harm subject to basic requirements

3

Institutional Framework

Brazil's implementation strategy leverages existing regulatory bodies with expanded authority:

- National Data Protection Authority (ANPD) as primary supervisory body
- Integration with Brazil's General Data Protection Law (LGPD)
- CNJ Resolution 332/2020 specifically governing AI deployment in judicial systems
- Sectoral regulators providing domain-specific oversight

Brazil's approach is distinguished by its emphasis on human rights protection, transparency requirements, strict non-discrimination provisions, and mandatory human oversight for high-risk AI systems. This framework creates a comprehensive ecosystem for responsible AI development while attempting to minimize barriers to innovation.

Core Principles of Brazilian AI Regulation

Human Rights Protection

AI systems must respect fundamental rights guaranteed by the Brazilian Constitution, including dignity, equality, and non-discrimination. All deployments must undergo human rights impact assessments prior to implementation.

Transparency & Explainability

Organizations must provide clear information about AI use, basic functionality, and potential impacts. High-risk systems require technical documentation explaining algorithmic decision-making processes.

Non-discrimination

AI systems must not perpetuate or amplify discrimination based on protected characteristics. Regular bias audits are mandatory for high-risk applications, particularly in credit, employment, and public services.

Human Oversight

Meaningful human supervision is required for all high-risk AI systems. Fully autonomous decision-making is prohibited for determinations with significant legal or financial consequences for individuals.

The Brazilian regulatory framework demonstrates a sophisticated understanding of AI's societal impacts, creating accountability mechanisms while acknowledging the technical realities of different AI architectures. This balanced approach has garnered praise from both industry and civil society organizations as a model for emerging economies.

AI as a Corporate Governance Enabler

Strategic Applications in Corporate Governance

When properly implemented, AI systems offer unprecedented capabilities to strengthen corporate governance mechanisms and enhance compliance functions. Brazilian corporations are increasingly deploying sophisticated AI tools that transform governance from reactive to proactive:

1

Automated Compliance Monitoring

AI systems capable of continuously scanning internal communications, transactions, and operational data to identify potential regulatory violations before they escalate. These systems can process unstructured data at scale, detecting patterns invisible to traditional monitoring approaches.

2

Predictive Risk Assessment

Machine learning models that analyze historical compliance data to forecast emerging risks and allocate resources efficiently. These predictive systems have demonstrated significant improvement in risk identification compared to traditional methods.

3

Intelligent Whistleblower Systems

Natural language processing tools that analyze anonymous reports, categorize allegations, and prioritize investigations based on severity and credibility factors. These systems enhance detection while preserving reporter confidentiality.

4

Automated Contract Performance Tracking

AI systems that monitor contractual obligations, deadlines, and performance metrics in real-time, generating alerts for potential breaches or compliance issues before they materialize into litigation.

Case studies from leading Brazilian financial institutions demonstrate that AI-enhanced governance systems can reduce compliance incidents while decreasing monitoring costs. These dual benefits make AI integration a strategic imperative for corporations operating in highly

AI as a Legal Risk Vector

1. Data Protection Violations
2. Algorithmic Bias & Discrimination
3. AI Hallucinations & Factual Errors
4. Prompt Engineering Liability
5. Civil Liability & Damages Attribution

Despite their benefits, AI systems introduce novel legal risks that corporations must systematically address. Brazilian courts have begun developing jurisprudence around AI-related harms, creating precedents that shape corporate liability.

Data Protection Risk

AI systems frequently process massive datasets containing personal and sensitive information. Under Brazil's LGPD, such processing requires explicit legal basis and comprehensive Data Protection Impact Assessments (DPIAs). Recent ANPD enforcement actions have targeted AI deployments that failed to establish proper legal grounds for data processing or conducted inadequate impact assessments.

Algorithmic Bias Risk

Machine learning systems trained on historical data inherently risk perpetuating structural biases related to gender, race, socioeconomic status, and other protected characteristics. Brazilian courts have begun recognizing algorithmic discrimination claims, particularly in employment and credit contexts. These cases carry significant liability exposure and severe reputational damage.

Hallucination & Prompt Liability

Generative AI systems can produce convincing but factually incorrect outputs. Brazilian courts are actively developing theories of liability that distribute responsibility among AI developers, prompt engineers, and corporate deployers. The emerging standard suggests that organizations cannot disclaim responsibility for AI outputs they incorporate into business processes.

Emerging Legal Risks in AI Deployment

1 Unclear Civil Liability Framework

The Brazilian legal system continues to evolve its approach to AI liability attribution. Current jurisprudence suggests movement toward a shared responsibility model between developers and deployers, with greater liability falling on the party with greater control over the specific risk factor that materialized. This uncertainty creates significant exposure for corporations integrating AI into critical processes.

2 Explainability Deficiencies

The "black box" nature of many advanced AI systems fundamentally conflicts with legal requirements for explainable decision-making. Brazilian courts have consistently held that inability to explain algorithmic determinations undermines due process and legal defense opportunities. This is particularly problematic for AI applications in credit scoring, employment decisions, and resource allocation.

Regulatory trend: The National Council of Justice Resolution 332/2020 and 615/2015 explicitly requires judicial AI systems to provide "clear explanations in natural language" for their recommendations - a standard increasingly applied to private sector deployments.

3 Transparency Failures

Brazilian consumer protection law (CDC) and the LGPD establish robust transparency requirements regarding automated processing. Organizations that deploy AI systems without proper disclosure face substantial liability under theories of bad faith, information duty violations, and consumer rights infringement.

Enforcement example: The Brazilian Consumer Protection Agency (PROCON) issued record fines to three major retailers in 2023 for undisclosed use of AI in customer service interactions, establishing that AI use must be affirmatively disclosed.

These evolving legal risks demonstrate why proactive AI governance is essential. Organizations operating in Brazil must establish comprehensive oversight mechanisms that address these specific risk vectors before deployment rather than responding to litigation after harm occurs.

The Rise of the Chief AI Officer (CAIO)

A New Corporate Leadership Role

In response to the complex intersection of technical, ethical, and legal considerations surrounding AI deployment, Brazilian corporations are increasingly establishing dedicated executive positions focused exclusively on AI governance. This emerging C-suite role serves as a critical bridge between traditionally siloed organizational functions:

Legal Compliance

Ensuring AI systems adhere to evolving regulatory requirements and anticipating emerging legal risks before deployment.

Technical Oversight

Evaluating architectural decisions, data sources, and technical safeguards against established risk parameters

Core CAIO Responsibilities

- Developing organization-wide AI ethics policies and implementation guidelines
- Conducting comprehensive algorithmic audits for bias, performance, and compliance
- Reviewing third-party AI systems before integration into corporate infrastructure
- Establishing transparency and explainability standards for all AI deployments
- Creating incident response protocols for AI failures or unintended consequences
- Managing AI risk registers and mitigation strategies
- Liaising with regulatory authorities on AI compliance matters
- Delivering executive education on AI capabilities and limitations

Brazilian market trend: It is expeced that around 40% of Brazilian companies with over 5,000 employees have established formal AI Ethics Committees, appointing dedicated CAIOs with direct board reporting lines.

Practical Structure of AI Compliance in Brazil

LGPD Compliance Foundation

Brazil's General Data Protection Law (LGPD) establishes fundamental requirements for lawful AI development and deployment:

- **Purpose Limitation:** AI systems must process data only for specified, legitimate purposes
- **Data Minimization:** Only essential data should be collected and retained
- **Security Measures:** Technical and organizational safeguards must protect AI training and operational data
- **Legal Basis:** All processing must have explicit legal grounds (consent, legitimate interest, etc.)

Contractual Governance

Brazilian organizations have developed sophisticated contractual frameworks for AI governance:

- Vendor assessment protocols for third-party AI providers
- Specific AI ethics clauses in procurement contracts
- Liability allocation provisions for AI-related harms
- Transparency requirements for algorithm updates and changes
- Audit rights for high-risk AI deployments

Internal Policies & Procedures

Effective governance requires comprehensive internal controls:

- Mandatory AI risk mapping before deployment
- Technical review procedures for AI systems
- Regular training for development and deployment teams
- Incident response protocols for AI failures
- "Privacy by Design" principles embedded in development lifecycle

Brazilian financial institutions have led the development of these governance frameworks, often exceeding regulatory requirements to establish industry best practices. Their approach emphasizes documentation, traceability, and human oversight throughout the AI lifecycle, creating auditable evidence of compliance efforts that can be presented in regulatory or judicial proceedings.

Case Study: AI Governance in Brazilian Banking

Itaú Unibanco's AI Governance Framework

Brazil's largest private bank has implemented a comprehensive AI governance structure that has become a reference model for financial institutions across Latin America. The framework addresses both the opportunities and risks of AI deployment in a highly regulated environment. (https://forbes.com.br/forbes-tech/2025/02/itau-unibanco-ingressa-no-instituto-de-ia-centrada-no-humano-de-stanford/)

Centralized AI Registry

All AI systems are cataloged in a central registry with detailed documentation of their purpose, data sources, algorithmic architecture, and risk classification. No AI system can enter production without registration and appropriate approval based on risk level.

Three-Tiered Approval Process

Low-risk systems require departmental approval, medium-risk systems require review by the AI Ethics Committee, and high-risk systems require executive board approval with documented risk mitigation measures.

Mandatory Explainability Standards

All customer-facing AI systems must be capable of generating human-readable explanations for their decisions, particularly for credit determinations and fraud detection outcomes.

Results & Regulatory Response

Itaú's proactive governance approach has yielded significant benefits:

Judiciary's Approach to AI Governance

CNJ Resolution 332/2020: The Judicial AI Framework

The National Council of Justice (CNJ) established Brazil's first comprehensive AI governance framework through Resolution 332/2020, which regulates the development and use of artificial intelligence within the judicial system. This pioneering regulation has become influential beyond the courts, providing guidance for corporate governance structures.

Key provisions of Resolution 332/2020, 615/2025, include:

- Mandatory transparency regarding the use of AI in judicial processes
- Requirement for human oversight of all AI-generated recommendations
- Explainability standards for algorithmic decisions affecting legal rights
- Prohibition of "black box" systems for consequential determinations
- Regular auditing requirements for bias and accuracy
- Preservation of human dignity and procedural guarantees

Emerging Judicial Precedents

Brazilian courts have begun developing jurisprudence on AI-related claims that establish important principles for corporate governance:

1 Shared Liability Principle

Courts have consistently rejected attempts to shift blame entirely to AI systems, holding that organizations deploying AI remain responsible for its outputs

Strategic Recommendations & Conclusion

Establish Corporate AI Governance Program

Develop a comprehensive governance framework that addresses the full AI lifecycle from conception through retirement. The program should include clear approval processes, risk assessment methodologies, documentation requirements, and incident response protocols.

This framework should be formally adopted at the board level and integrated into existing risk management structures to ensure consistent application across the organization.

Appoint AI Leadership

Designate executive responsibility for AI governance through either a dedicated Chief AI Officer or expanded mandate for existing leadership. This role should have sufficient authority and independence to effectively evaluate AI risks and benefits.

For organizations with extensive AI deployments, consider establishing a cross-functional AI Ethics Committee with representatives from legal, technical, business, and ethics backgrounds.

Implement Algorithmic Impact Assessments

Develop a systematic methodology for evaluating potential impacts of AI systems before deployment, with particular focus on human rights implications, potential discrimination, and regulatory compliance.

These assessments should be living documents updated throughout the AI lifecycle as systems evolve and use cases expand beyond initial parameters.

Adopt Risk-Based Approach

Align with Brazil's emerging regulatory framework by implementing tiered governance based on risk classification. This approach allows for appropriate oversight without unnecessarily burdening low-risk applications.

Document risk classification decisions and revisit classifications periodically as both systems and societal understanding of AI risks evolve.

Critical Insight

"In Brazil, we've learned that innovation without accountability leads to litigation. AI governance must start within the company – before the law demands it."

The Brazilian experience demonstrates that organizations which proactively address AI governance challenges not only mitigate legal risk but also gain competitive advantages through improved stakeholder trust and operational efficiency. By establishing robust governance frameworks now, corporations can help shape emerging regulations rather than merely reacting to them.