WHY GOVERN AI IN A SCENARIO OF REGULATORY UNCERTAINTY?

- Why govern AI in the scenario of regulatory uncertainty?
- The environment is regulated and requires attentionEnforcement is already a reality in Brazil
- AI as a new strategic pillar in corporate ESG
- Governing AI is about improving innovation conditions and operational efficiency
- What are the risks that can arise from a lack of AI governance?
- Framework for governing AI against a backdrop of regulatory uncertainty

TABLE OF CONTENTS

ABOUT US

Vainzof, Lima e Karassawa Advogados (VLK) sees the law as a tool to drive innovation, business success, and a more prosperous and just society.

We actively participate in the construction of regulatory frameworks and hundreds of innovative projects, which allows us to anticipate trends and generate legal security to make business viable in the following practice areas:

- Ethical Governance and Data Protection;
- Artificial Intelligence;
- Cybersecurity and Incident Response;
- Creative Economy, Legal Marketing and Intellectual Property;
- Legal Design and Visual Law;
- Advocacy and Strategic Technology Regulation;
- Strategic Litigation.

COMUNICACAO@VLKLAW.COM.BR

Why govern AI in a scenario of regulatory uncertainty?

Artificial Intelligence (AI) governance transcends simple legal compliance, positioning itself as a strategic advantage for companies that want to lead in a dynamic and ever-changing regulatory environment. In addition, robust governance promotes operational efficiency, facilitates innovation by ensuring that the business strategy is aligned with the ethical and responsible use of technology, and strengthens the trust of customers and business partners, consolidating the company's reputation in the market.

Although Brazil does not yet have specific legislation for AI, the current legal scenario already imposes requirements and guidelines that directly impact business operations.

1. The environment is regulated and requires attention

It is a misconception that AI is unregulated—existing laws already apply! Companies that develop and use AI operate in a context in which laws such as the Civil Code, the Consumer Protection Code ('CDC'), the General Data Protection Law ('LGPD'), and specific sectoral regulations establish parameters that cannot be ignored.

The LGPD, for example, establishes a series of principles and rights that, in general, align with international standards for responsible AI, such as those provided for by the OECD[1], at least when AI systems involve the processing of personal data. For example, it is impossible to comply with the principles of transparency and the rights provided for in article 20 of the LGPD without observing the OECD principle of "transparency and explainability". These requirements make it essential to implement AI governance practices to mitigate legal and reputational risks.

Organizations that already prioritize AI governance have a greater ability to meet these regulatory requirements, while demonstrating to customers and business partners a commitment to ethics and responsibility. AI systems that are aligned with good practices and international standards (such as ISO standards and the NIST AI RMF) will present competitive differentials, better navigating the complex regulatory landscape.

[1] https://oecd.ai/en/ai-principles

2. *Enforcement* is already a reality in Brazil

Despite the absence of specific AI legislation, companies are already subject to active regulatory scrutiny. In addition, court decisions and administrative inspection processes related to the use of AI are already shaping market practices.

In this context, the **National Data Protection Authority** ("ANPD") has initiated administrative proceedings against technology companies in Brazil to investigate their practices related to the development and use of generative AI systems. The ANPD's concern with the regulation of the subject is evidenced by its recent subsidies on the subject, as well as its regulatory agenda for the 2025-2026 biennium[1], which includes the establishment of interpretative parameters for the application of article 20 of the LGPD, which provides for the right to review automated decisions.

The **National Telecommunications Agency ("ANATEL")** has also intensified its mission to regulate and supervise the use of AI systems in the telecommunications sector. Through Letters sent to technology companies such as OpenAI, Google, and Microsoft, ANATEL explored the implications of the use of generative AI in the sector, including the cybersecurity risks of such systems[2]. In its goals for 2025,

ANATEL provides for the creation of specific standards for the use of technology in telecommunications networks, reinforcing its commitment to innovation, efficiency, and consumer protection[3].

Likewise, the **Superior Court of Justice ("STJ")** has already established relevant precedents on the subject. In Topic 710[3], for example, the court established the minimum information requirements for credit profiling. In REsp 2.135.783-DF[4], the court recognized the right of app drivers to obtain explanations about de-

accreditation, reinforcing the importance of ethical practices in the application of AI.

Executives who wait for a specific regulation may be caught off guard by legal interpretations based on existing rules. That's why preparedness is crucial: investing in AI governance now is more efficient and less costly than reacting to sanctions or image crises in the future.

[1] https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-agenda-regulatoria-2025-2026

[2] https://teletime.com.br/24/07/2024/anatel-questiona-google-microsoft-e-openai-sobre-riscos-de-ia-generativa/

[3] https://www.gov.br/anatel/pt-br/assuntos/noticias/anatel-registra-avancos-na-abordagem-do-tema-inteligencia-artificial

[4] https://processo.stj.jus.br/repetitivos/temas_repetitivos/pesquisa.jsp?novaConsulta=true&tipo_pesquisa=T&cod_tema_inicial=710&cod_tema_final=710

[5] https://scon.stj.jus.br/SCON/pesquisar.jsp?b=ACOR&livre=%28RESP.
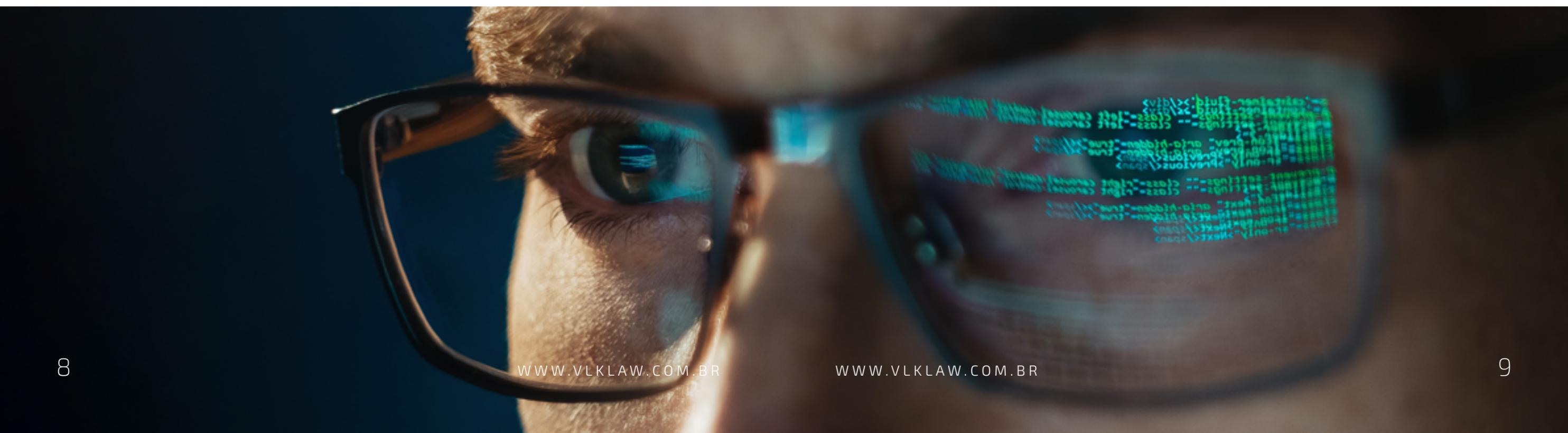
3. AI as a new strategic pillar in Corporate ESG

AI governance is rapidly emerging as a fundamental pillar for businesses committed to responsible and sustainable operations. Like environmental and compliance practices, which have evolved into global standards regardless of legal requirements, AI governance transcends regulatory boundaries.

Companies and executives already understand that getting ahead of robust AI governance is more than a matter of compliance; It is a strategic requirement to ensure stakeholder confidence and resilience in increasingly demanding markets.

DID YOU KNOW?

According to a Cisco survey conducted in 2023[1], 62% of consumers expressed concern about the use of artificial intelligence (AI) by companies, and 60% said they had already lost trust in organizations due to this use. Despite this, 48% of respondents believe that AI has the potential to improve their lives. However, the majority (77%) highlight the importance of organizations being responsible in the use of this technology. To mitigate these concerns, 72% of consumers stated that they would feel more comfortable if AI applications were audited to avoid bias, while 75% want greater transparency and human participation in decision-making processes involving AI.

Just as advanced environmental practices have become a competitive differentiator and an ethical obligation, responsible AI management is emerging as an indispensable component of corporate responsibility. Executives should consider AI governance as an integral part of their ESG strategies. This means adopting principles of transparency, safety, and ethics in the development and application of AI technologies, even before specific regulations are enacted. Companies that neglect AI governance risk losing credibility and competitiveness in a global market that prioritizes responsibility and ethical innovation.

[1] https://www.cisco.com/c/dam/global/pt_br/products/security/pdfs/consumer-privacy-report-2023.pdf

4. Governing AI is about improving innovation conditions and operational efficiency

The era of AI has already begun and, according to Gartner, by 2026, 80% of organizations will use general-purpose AI application programming models or interfaces or implement solutions with these technologies[1].

In such a dynamic scenario, ensuring efficient processes in the implementation and management of AI solutions is crucial for the competitiveness of companies. The adoption of AI governance practices today results in better results in the future, helping to avoid, for example, unnecessary expenses with redundant solutions, investments in projects that are incompatible with current regulations, among other risks.

DID YOU KNOW?

In this sense, Gartner predicts that, by 2026, organizations that adopt AI ethically and responsibly will experience a 50% improvement in business results and user acceptance[2].

Investing in AI governance now is to ensure more effective results that are in line with legal and market requirements in the future.

[1] https://tiinside.com.br/23/10/2023/gartner-preve-que-mais-de-80-das-empresas-usarao-apis-de-inteligencia-artificial-generativa-ate-2026/

[2] https://valor.globo.com/opiniao/coluna/a-confianca-digital-e-o-custo-da-inacao.ghtml

5. What are the risks that can arise from a lack of AI governance?

The absence of adequate AI governance measures can generate numerous risks, many of which have significant impacts for those affected. In addition, the materialization of these risks may imply a violation of legal and regulatory rules in force, especially the LGPD. While the specific risks vary depending on the application of AI, we highlight some of the most common risks below:

Lack of Data Quality:

it can occur when the AI result has a low performance or accuracy, implying unfair, inappropriate or unsatisfactory results or decisions. It can be seen as a violation of the principle of data quality, since the UK Data Authority (ICO) understood that it covers the statistical accuracy of AI[1].

Discriminatory Biases:

or violation of equity, may occur when there is evidence of unlawful discrimination in the results generated, reflecting stereotypes or discriminatory patterns, or the existence of failures in the design that makes it difficult or impossible for certain groups of people to use AI – either due to issues related to accessibility or the inadequacy of AI for that demographic group. This risk may imply a violation of the principle of non-discrimination, of the LGPD.

Data Exposure:

is the violation of confidentiality of personal data, business secrets, know-how, or other sensitive information, as a result of the AI solution, either by system failures or cyberattacks. It may imply a violation of the LGPD's principle of security.

Violation of third party rights:

it may occur when there is a violation of intellectual property or personality rights of third parties, due to the development or use of the AI solution. It may imply the violation of intellectual property rules, such as the Copyright Law, Software Law, and the Industrial Property Law.

Lack of transparency:

it can occur in cases of failure to provide affected persons with appropriate information regarding the development or application of AI solutions. It may imply a violation of the principle of transparency, provided for in the LGPD, if the data subject is not informed in advance about the use of their data to train or apply AI[2].

Lack of Explainability:

is the inability to provide affected people with appropriate and understandable information about how the AI solution reached a particular output. It may imply a violation of the provisions that deal with the provision of information on automated decision-making provided for in the LGPD, or even the right to information.

Loss of Human Autonomy:

it is the risk of reducing the freedom of the human person to machines, as well as being subject to inappropriate decisions. It may imply a violation of the provisions that deal with the review of automated decisions provided for in the LGPD when the organization does not adopt a human review procedure.

[1] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/what-do-we-need-to-know-about-accuracy-and-statistical-accuracy/
[2] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/how-do-we-ensure-fairness-in-ai/

6. How to govern AI in a scenario of regulatory uncertainty?

In a scenario where regulation is still constantly evolving, having solid governance based on internationally recognized good practices is essential. This ensures that your governance structure is prepared to adapt to future regulations in an agile, efficient and at the lowest possible cost.

To support business success, VLK has developed a proprietary AI governance framework, inspired by the main global standards, such as NBR ISO 42001:2024, NIST AI RMF, IAPP-AIGP, the European AI Act, and the current text of PL No. 2,338/2023.

At VLK, we understand that a successful and beneficial AI governance program is one that is integrated into the business strategy and governance structure that already exists. Our framework is structured in six strategic phases, which ensure a continuous, robust, sustainable implementation in line with market requirements:

1. Definition of the AI Strategy:

for an AI governance program to be successful and benefit the organization, it is essential that it is integrated with the business strategy and the existing digital governance structure to identify synergies. This stage aims to raise awareness of the Executive Board on the importance of AI Ethical Governance and its strategic impact and the alignment of the strategy with corporate objectives.

2. Inventory of AI Applications and Legal Requirements:

with the AI strategy defined, it becomes essential to understand the governance requirements required or expected of the organization. To do this, it is necessary to identify the planned or ongoing AI projects, classify, as well as analyze the organization's position as an AI agent at each stage of the system's lifecycle, through the detailed inventory of AI solutions and their preliminary evaluation. This analysis makes it possible to align governance practices to be implemented with the specific concrete needs of each organization, promoting greater control and efficiency.

3. Structuring AI Governance:

with the expected governance defined, it is essential to plan how to achieve this desired level, either globally or for each specific solution. This requires identifying the "gaps" that the organizational structure and AI projects need to fill, as well as aligning the governance structure responsible for leading this process, including defining roles, responsibilities, and criteria for risk management. This planning directs efforts to reduce gaps and ensure that governance is fully integrated and operational.

4. Documentation of AI Policies:

with the governance structure aligned, it is necessary to transform it into binding policies, standards, and models applicable to the entire organization after structuring the governance. This stage aims to standardize the governance structure, attributing appropriate powers, guarantees, and responsibilities to the different agents involved in the AI life cycle, ensuring clarity, uniformity, and adherence to the established principles and objectives.

5. Execution of Compliance Plans for Existing Applications:

with the governance structure standardized and officially established, it is time to apply it to correct the gaps identified in the organization's AI projects. Drafting and reviewing relevant contracts and documents, such as acceptable use policies, conducting Algorithmic Impact Assessments for high-risk AI solutions, and ensuring adequate transparency for people impacted by AI, promoting compliance and trust in processes. The objective of this phase is to correct any gaps identified in the organization's AI projects.

6. Acculturation, Active Maintenance, and Continuous Evaluation:

the AI governance structuring plan has been executed, but, like any governance system, it must be continuously reinforced and improved. For this, it is essential to implement acculturation actions (such as training and visual guides), develop KPIs for constant monitoring, and define requirements to be considered in future audits, among other measures. These actions ensure that AI governance remains aligned with the organization's needs and technological advancements and is continuously reinforced and improved with the aim of ensuring its sustainability.

E-book " Why govern AI in a scenario of regulatory uncertainty?", March, 2025.