JeDEM 18(2): 1-34, 2026
ISSN 2075-9517
http://www.jedem.org
Date of submission: 16.11.2025
Date of acceptance: 10.08.2026
Article DOI: 10.29379/jedem.v18i2.1173

Data Protection in AI-Driven Environments: The Model for Mapping Institutional Consciousness

André Afonso Silva

Author ORCID Nr: 0009-0008-2007-293X
Universidade do Estado do Rio de Janeiro (UERJ), Rio de Janeiro, RJ, Brazil
andre.silva@uerj.br

Abstract: Artificial intelligence (AI) systems increasingly shape organisational decision-making, yet, the institutional capacities required to align these technologies with Brazil's General Data Protection Law (LGPD) remain uneven. This article argues that many organisations, whether public or private, face institutional consciousness gaps, defined here as structural, cognitive, and cultural deficiencies that hinder their ability to understand and operationalise the ethical and legal implications of data-driven systems. Drawing on a theoretical-analytical approach, the study identifies how these gaps emerge in AI governance and how they distort accountability and normative interpretation. Building upon this analysis, the article introduces the Model for Mapping Institutional Consciousness (MMIC), a conceptual framework designed to support diagnostic assessment and strengthen governance practices in AI-mediated environments. The study argues that without addressing these internal deficiencies, organisations tend to reproduce formal compliance without substantive alignment with LGPD principles, resulting in governance structures that appear consistent but fail to adequately protect data subjects.

Keywords: Artificial intelligence; Institutional consciousness; AI governance; LGPD compliance; Organisational accountability;

Acknowledgement: I thank Diego Aguiar and Jennifer Kinne for their careful reading of an earlier version of this manuscript and for their comments.

Statement on the use of AI: During the preparation of this work, the author used Claude (Anthropic) in order to review the manuscript against the reviewers' comments, draft and edit passages of text, structure Table 2, prepare Figure 3, and compile bibliographic entries for sources already cited in the text. After using this tool/service, the author reviewed and edited the content as needed and takes full responsibility for the content of the published article.

 CC BY-NC 4.0 DEED Attribution-NonCommercial 4.0 International, 2026

1. Introduction

The enactment and consolidation of Law No. 13.709/2018, the Brazilian General Data Protection Law (Lei Geral de Proteção de Dados Pessoais – LGPD), constituted a major legal milestone in the national regulatory landscape. Inspired by the European General Data Protection Regulation (GDPR), the LGPD expanded the scope of privacy protections and anchored them within a context of rapid technological transformation. However, the existence of a comprehensive data protection statute does not, by itself, ensure effective institutional implementation.

Recent experience shows, that many Brazilian public and private organisations struggle to internalise the LGPD's principles in their everyday processes. The challenge lies not only in understanding the legal requirements, but in translating normative principles into institutionalised governance practices supported by a culture of governance, accountability, and ethical responsibility.

The reflection developed in the present work, originated from an emblematic situation commonly found in organisations that process sensitive personal data: an institutional disconnect between decision-makers and those responsible for executing data processing activities. During an institutional AI implementation project conducted at a Brazilian university, it became evident that the adoption of AI tools was occurring at the individual level, outside the scope of institutional contracting, and therefore outside the perimeter that institutional governance is designed to observe. Although context-specific, this case illuminated the procedural and conceptual gap that frequently separates the normative expectations of the LGPD from organisational reality.

This experience served as the starting point for the theoretical proposition advanced here. This study argues that such inconsistencies do not stem merely from operational failures or limited knowledge of the law. Instead, it reveals a deeper phenomenon: institutional consciousness gaps, understood as institutional deficiencies affecting the organisation's ability to perceive, interpret, and act upon the ethical and legal implications of personal data processing in environments increasingly mediated by AI.

Recent developments in AI governance further reinforce this institutional challenge. Regulatory and governance frameworks, such as the European Union AI Act and ISO/IEC 42001, increasingly emphasise that effective AI governance depends not only on technical compliance mechanisms but also on organisational structures capable of embedding accountability, risk management, transparency, and continuous oversight into institutional decision-making. Collectively, these developments reinforce the argument advanced in this study that legal compliance alone is insufficient unless accompanied by broader institutional preparedness.

The purpose of this study is to provide a conceptual foundation for interpreting these gaps and to introduce a maturity-oriented framework capable of supporting institutional diagnosis and governance assessment within organisations. By proposing MMIC, the article seeks to contribute to debates on AI governance and data protection by highlighting that substantive compliance depends not only on procedures, but on the institution's institutional reflexive capacity to sustain responsible and rights-aligned technological decisions.

 CC BY-NC 4.0 DEED Attribution-NonCommercial 4.0 International, 2026

The remainder of this study is structured as follows: Section 2, presents the theoretical background, including LGPD fundamentals, AI governance challenges, and the conceptual basis of institutional consciousness. Section 3, outlines the theoretical–analytical approach adopted. Section 4, details the core features of institutional consciousness gaps and their manifestations in algorithmic environments. Section 5, discusses the MMIC as a conceptual instrument for organisational diagnosis. Section 6, offers concluding reflections and identifies directions for future research.

This study develops a conceptually derived framework through the analytical synthesis of institutional governance, AI governance, and data protection literature. Rather than providing empirical validation, it advances a theoretically grounded model intended to support future empirical investigation and institutional assessment. Accordingly, the MMIC is intended as an analytical governance framework rather than a regulatory compliance checklist.

Background / Literature Review

1.1. Data Protection, Normative Foundations and the Limits of Formal Compliance

The LGPD, inspired by the GDPR, established a comprehensive legal framework that reorganises institutional responsibilities for the processing of personal data. Beyond creating obligations, the LGPD expresses a normative architecture grounded in principles, such as purpose limitation, adequacy, necessity, transparency, non-discrimination, security, prevention, and accountability. These principles form a coherent system whose effectiveness depends on institutional internalisation, not merely procedural adherence.

Although the LGPD is clear in its structure and definitions, the operationalisation of its principles encounters persistent obstacles in many Brazilian institutions. The distance between the normative text and institutional practices illustrates what Doneda (2021) describes as the tension between formal compliance and substantive protection. Legal requirements may be acknowledged, yet not fully understood in their conceptual depth, resulting in organisational behaviours that satisfy documentation demands but fail to sustain ethical, secure, and rights-oriented processing of personal data.

This disconnect becomes more problematic in public-sector contexts, where legal compliance intersects with constitutional duties, democratic legitimacy, and citizens' rights. This study proposes that limited interpretive maturity can amplify structural inadequacies, where institutions lack the internal conditions to give concrete meaning to principles, such as necessity and non-discrimination. In such cases, data-protection frameworks risk remaining formally acknowledged but weakly internalised, particularly when technological systems mediate decision-making (Meyer & Rowan, 1977; Brunsson, 2002; EDPB, 2022).

The literature on regulatory implementation corroborates these patterns. Parker and Braithwaite (2003) note that compliance tends to deteriorate when organisations face normative ambiguity, operational fragmentation, or cultural resistance. These conditions are precisely those identified in

 CC BY-NC 4.0 DEED Attribution-NonCommercial 4.0 International, 2026

many Brazilian organisations dealing with personal data: a landscape where the law is recognised, but the ability to act upon it responsibly remains deficient.

Such deficits provide the foundation for this article's central argument: that institutional consciousness gaps emerge not from ignorance of the law, but from the lack of interpretive, structural, and cultural capacities necessary for transforming normative expectations into coherent and coordinated organisational practices.

1.1. Artificial Intelligence, Algorithmic Opacity and Organisational Vulnerabilities

The integration of AI into public administration intensifies the challenges of data protection. AI systems process vast quantities of information, generate predictions and classifications, and influence decisions in ways that can be difficult to interpret, audit, or contest. Algorithmic opacity — whether stemming from model complexity, proprietary constraints, or inadequate documentation — creates what Burrell (2016), identified as three forms of opacity: intentional, technical, and epistemic.

Taken together, these characteristics shift the governance challenge from merely regulating technological artefacts to strengthening the institutional capacity required to oversee their responsible deployment.

In the Brazilian scenario, these dimensions of opacity intersect with structural weaknesses in public institutions, creating an environment in which algorithms are often implemented without sufficient institutional reflexivity. Pelizza (2020), points out that algorithmic systems tend to "embed institutional histories," shaping classifications and decisions according to prior organisational logics, biases, and blind spots. When institutions lack the capacity to examine these dynamics critically, opacity becomes not merely a technical condition but an organisational vulnerability.

International bodies have emphasised the need for robust governance frameworks to address these risks. The OECD's AI Principles (2023), stress transparency, robustness, and accountability as prerequisites for trustworthy AI. UNESCO (2021), highlights similar concerns, calling for institutions to cultivate, not only technical safeguards but also ethical awareness and cultural maturity.

The LGPD aligns with these international frameworks, yet its implementation confronts the same institutional limitations noted by scholars of public administration: fragmented decision-making, informal delegation, and low interpretive capacity. These weaknesses undermine the ability to evaluate algorithmic risks, anticipate discriminatory outcomes, or ensure that automated decisions respect constitutional principles.

In environments where AI is adopted without critical evaluation, institutions often default to a reactive logic. Problems only surface after harm occurs, rather than being prevented through structured governance. This reactive pattern reflects a broader absence of institutional consciousness — an inability to perceive how algorithmic practices interact with legal obligations, organisational processes, and social consequences.

 CC BY-NC 4.0 DEED Attribution-NonCommercial 4.0 International, 2026

1.1. Organisational Culture, Reflexivity and the Concept of Institutional Consciousness

Organisational culture plays a central role in how institutions handle data protection and AI governance. As Choo (2003), points out, organisations don't just act on what they know; they act on how they interpret and make sense of their environment. But when institutions lack reflexivity (the ability to examine their own practices, question their assumptions, and think through consequences), they often fall back on informal routines that clash with their formal structures.

Brunsson (2002), describes this as the "organisation of hypocrisy," in which talk, decisions, and actions diverge systematically. Institutions declare commitments to transparency, rights protection, and compliance, yet everyday operations follow different logics. This divergence is not necessarily intentional; it often arises from structural disconnects, informal delegation, and the absence of shared interpretive frameworks.

The concept of institutional consciousness, as developed in this article, builds upon these insights. Institutional consciousness refers to the organisation's collective ability to perceive, interpret, and respond coherently to legal, ethical, and social implications of personal data processing. It encompasses:

- - the depth of normative understanding,
- - internal coordination structures,
- - alignment between strategic decisions and operational practices,
- - reflexive awareness of technological risks, and
- - ethical commitment embedded in the institutional culture.

Where these conditions are absent, organisations experience consciousness gaps: deficits in awareness and interpretation that undermine the substantive implementation of the LGPD.

Merton's classic analysis (1936), of unintended consequences resonates with this problem. When institutions act without interpretive clarity or structural alignment, well-intentioned decisions may produce harmful outcomes. In AI-mediated environments, the stakes are even higher: opacity amplifies uncertainty, and decisions can affect large populations rapidly and irreversibly.

Reflexive capacity is, in this sense, a prerequisite for democratic oversight in digital governance. Without it, institutions lack the ability to foresee risks, audit algorithmic behaviour, or align technologies with constitutional principles. This reinforces the need to analyse how organisational culture shapes — positively or negatively — the capacity to implement the LGPD in a manner substantiated by rights-based commitments.

These perspectives collectively suggest that effective AI governance depends not only on organisational capabilities but also on the institutional capacity to recognise, internalise, and operationalise governance principles before regulatory deficiencies become visible. This analytical convergence

 CC BY-NC 4.0 DEED Attribution-NonCommercial 4.0 International, 2026

provides the conceptual basis for the construct of Institutional Consciousness developed in this study.

1.1. Institutional Consciousness Gaps: A Synthesis of Theoretical Contributions

The literature discussed above converges on a central insight: organisations do not fail to comply with data protection obligations merely because they lack technical solutions. They fail because they lack the institutional capacities required to perceive and interpret the ethical, legal, and social implications of their data practices — capacities that are essential when AI mediates decisions that affect individuals and collectives.

Rather than merely juxtaposing the preceding theoretical perspectives, this synthesis identifies their analytical convergence around a common institutional problem: organisations frequently possess formal governance structures without developing the institutional awareness required to implement them substantively. It is precisely this convergence that motivates the formulation of Institutional Consciousness as an independent analytical construct.

Across regulatory theory (Parker & Braithwaite, 2003), organisational sociology (Brunsson, 2002), information culture (Choo, 2003), AI ethics (Floridi & Cowls, 2019), and analyses of algorithmic opacity (Burrell, 2016), a consistent theme emerges: institutions act according to what they understand, not according to what formal rules demand. When interpretive frameworks are weak or fragmented, institutions reproduce inconsistent practices that undermine the substantive goals of the law.

These insights illuminate the conceptual basis for the central phenomenon to this article: institutional consciousness gaps. Such gaps arise when an institution:

- - recognises its legal obligations,
- - possesses documentation and formal structures,
- - (but) lacks the internal interpretive, reflexive, and cultural resources to transform the normative framework into coherent action.

The LGPD presupposes a level of institutional maturity, in which principles are actively interpreted, risks are anticipated, and decisions are evaluated through legal-ethical lenses. This study proposes that organisations may remain at the early stages of conceptual understanding, where compliance is reduced to the production of documents, rather than the cultivation of reflexive governance. As Doneda (2021), notes, “the efficacy of data protection frameworks depends less on textual clarity and more on the institutional capacity to act upon principles in concrete contexts.”

In AI-mediated environments these deficits expand. The opacity, unpredictability, and speed of algorithmic systems impose new cognitive and ethical demands on organisations, requiring them to:

- - comprehend how algorithmic processes interact with data subjects’ rights,

 CC BY-NC 4.0 DEED Attribution-NonCommercial 4.0 International, 2026

- - anticipate structurally embedded risks,
- - evaluate the implications of automated decisions,
- - maintain institutional accountability even when decision paths are not transparent.

Organisations that lack the reflexive capacity to meet these demands exhibit institutional consciousness gaps marked by:

- - limited normative depth (superficial interpretation of LGPD principles),
- - fragmented decision-making (disconnects between controllers and operators),
- - structural complacency (belief that documentation equals compliance),
- - cultural inertia (resistance to rethinking routine practices),
- - reactive governance (responses only after harm or external pressure).

In public-sector contexts, the consequences are particularly severe. Democratic governance requires institutions that can, not only process information but also, interpret it responsibly. Without this interpretive capacity, public administration becomes vulnerable to reproducing asymmetries and opaque decision-making processes that citizens cannot contest or understand (Janssen & Kuk, 2016), including the reproduction of discriminatory patterns embedded in algorithmic systems (Noble, 2018).

Accordingly, the literature review does not merely establish the theoretical background of the study; it also provides the analytical basis from which the MMIC is conceptually derived.

1.1. Implications for the Implementation of the LGPD in AI-Mediated Public Administration

The theoretical synthesis above, reveals a crucial finding: the main obstacles to LGPD compliance in public-sector AI contexts are not technological, but institutional. They emerge from:

- - organisational structures that separate decision-making layers,
- - insufficient coordination between roles,
- - lack of awareness of algorithmic risks,
- - a culture oriented toward operational pragmatism rather than normative interpretation.

In many administrations, legal frameworks are sometimes adopted with symbolic enthusiasm while internal conditions remain unchanged, producing architectures that are formally adequate yet substantively weak—unable to evaluate automated decisions or to protect data subjects effectively (Meyer & Rowan, 1977; DiMaggio & Powell, 1983; Parker, 2002).

 CC BY-NC 4.0 DEED Attribution-NonCommercial 4.0 International, 2026

From the perspective of international governance frameworks, this mismatch signals a deeper deficit: institutions lack the maturity required for trustworthy AI adoption. OECD (2023) and UNESCO (2021), documents stress that trustworthy AI depends on:

- - institutional transparency,
- - internal accountability,
- - technical and ethical auditing mechanisms,
- - and reflexive governance structures.

When institutions lack these elements, the LGPD cannot fulfil its protective potential. Instead, formal compliance coexists with structural blind spots, and organisational weaknesses become amplified by algorithmic opacity.

This reinforces the central premise of this article: LGPD implementation requires institutional consciousness.

Without this, the organisation will remain trapped in cycles of:

- - fragmented decisions,
- - informal delegation,
- - inadequate oversight,
- - and symbolic compliance.

Such patterns, not only violate LGPD principles but also weaken public trust and democratic legitimacy, particularly when automated systems influence decisions related to public services and fundamental rights.

1.1. Transition to the Analytical Framework

The literature reviewed in this section provides the conceptual foundation for the analytical argument developed in the remainder of this article. The notion of institutional consciousness emerges as a theoretical construction capable of explaining why organisations — especially in the public sector — struggle to operationalise LGPD principles in AI-mediated contexts.

Building on this theoretical foundation, the next section explains the theoretical–analytical approach adopted in this study and the process through which the analytical insights identified throughout the literature were systematically integrated to derive the MMIC. This transition marks the shift from theoretical synthesis to framework development, establishing the analytical rationale underlying the proposed model.

 CC BY-NC 4.0 DEED Attribution-NonCommercial 4.0 International, 2026

Methodological Procedures

This study adopts a conceptual, theory-building design rather than an empirical or case-based one (Whetten, 1989). The choice is deliberate and methodologically grounded: the objective is to construct an analytical framework — the MMIC — capable of explaining a recurring class of institutional phenomena, not to test hypotheses against data drawn from a single organisation. Conceptual contributions of this kind are an established mode of scholarly inquiry, particularly in emerging governance domains where the phenomenon of interest — here, institutional consciousness gaps — has not yet been operationalised into measurable constructs. For this reason, the situated institutional episode reported in this article functions strictly as the analytical trigger that motivated the research problem; it is neither an empirical object of analysis nor evidence supporting the framework. Empirical validation of the MMIC, including the development and testing of measurement instruments, is identified as a necessary direction for subsequent research and lies explicitly outside the scope of the present contribution.

1.1. Framework derivation

The MMIC was developed through a conceptually driven analytical synthesis rather than through empirical induction. Accordingly, the objective of the present study is theory building rather than theory testing, providing a conceptually grounded framework intended to support subsequent empirical investigation. The objective of this process was not to generate findings from a specific organisational setting, but to integrate complementary theoretical perspectives capable of explaining why formal compliance with data protection requirements frequently fails to translate into effective institutional governance in AI-driven environments. The objective of this process was theory building rather than theory testing.

The derivation process was intentionally iterative rather than linear. As theoretical insights from the three literature domains were progressively compared, recurring governance tensions were continuously refined through analytical abstraction until they converged into a coherent institutional governance construct. This iterative movement between synthesis and abstraction ensured that the proposed framework reflected conceptual convergence rather than isolated theoretical propositions.

Three literature streams were deliberately selected because each addresses a distinct dimension of the governance problem while remaining insufficient on its own. The institutional governance literature explains how organisational structures, decision-making processes, accountability mechanisms, and institutional capacity influence governance outcomes. AI governance literature contributes principles related to transparency, explainability, accountability, human oversight, and risk management in increasingly autonomous technological environments. Data protection literature, particularly discussions surrounding the Brazilian General Data Protection Law (LGPD) and comparable international regulatory frameworks, provides the normative and legal perspective required to understand compliance obligations and institutional responsibilities. Considered independently, these bodies of knowledge illuminate only partial aspects of the governance challenge. Their integration offers a broader conceptual foundation for examining institutional preparedness for AI adoption.

 CC BY-NC 4.0 DEED Attribution-NonCommercial 4.0 International, 2026

The analytical synthesis consisted of an iterative process of comparing, integrating, and abstracting recurring concepts across these three domains. Rather than seeking convergence at the level of individual regulatory prescriptions or technological solutions, the analysis focused on identifying recurring institutional tensions repeatedly discussed throughout literature. Examples include the persistent gap between formal regulatory compliance and substantive organisational practices, fragmented governance responsibilities, insufficient institutional learning, weak accountability structures, and the absence of mechanisms capable of anticipating governance risks associated with AI deployment.

Accordingly, the MMIC should be understood as the outcome of theory integration rather than theory aggregation. Its analytical dimensions do not reproduce individual governance principles; instead, they synthesise recurring institutional patterns identified across the literature.

These recurring tensions were subsequently subjected to conceptual abstraction. Instead of treating them as isolated implementation problems, they were interpreted as manifestations of an underlying institutional condition concerning the organisation's capacity to recognise, internalise, and operationalise governance principles before regulatory deficiencies materialise. This abstraction process gave rise to the concept of **Institutional Consciousness,** understood as the degree to which governance principles become embedded within institutional structures, decision-making processes, and organisational practices.

Based on this iterative analytical synthesis, the dimensions composing the MMIC were derived as analytical categories representing complementary manifestations of institutional consciousness. The proposed maturity levels emerged from the recognition that institutional awareness develops progressively rather than dichotomously. Instead of representing organisational performance indicators, the maturity levels describe increasing degrees of institutional capability to anticipate governance risks, integrate regulatory principles into organisational routines, and translate formal compliance into substantive governance practices.

Figure 1, summarises the conceptual development process adopted in this study. Rather than emerging from empirical induction, the MMIC was derived through an iterative process of analytical synthesis integrating institutional governance, AI governance, and data protection literature. The figure illustrates how recurring institutional governance tensions were conceptually abstracted into analytical dimensions and subsequently organised into progressive maturity levels.

 CC BY-NC 4.0 DEED Attribution-NonCommercial 4.0 International, 2026

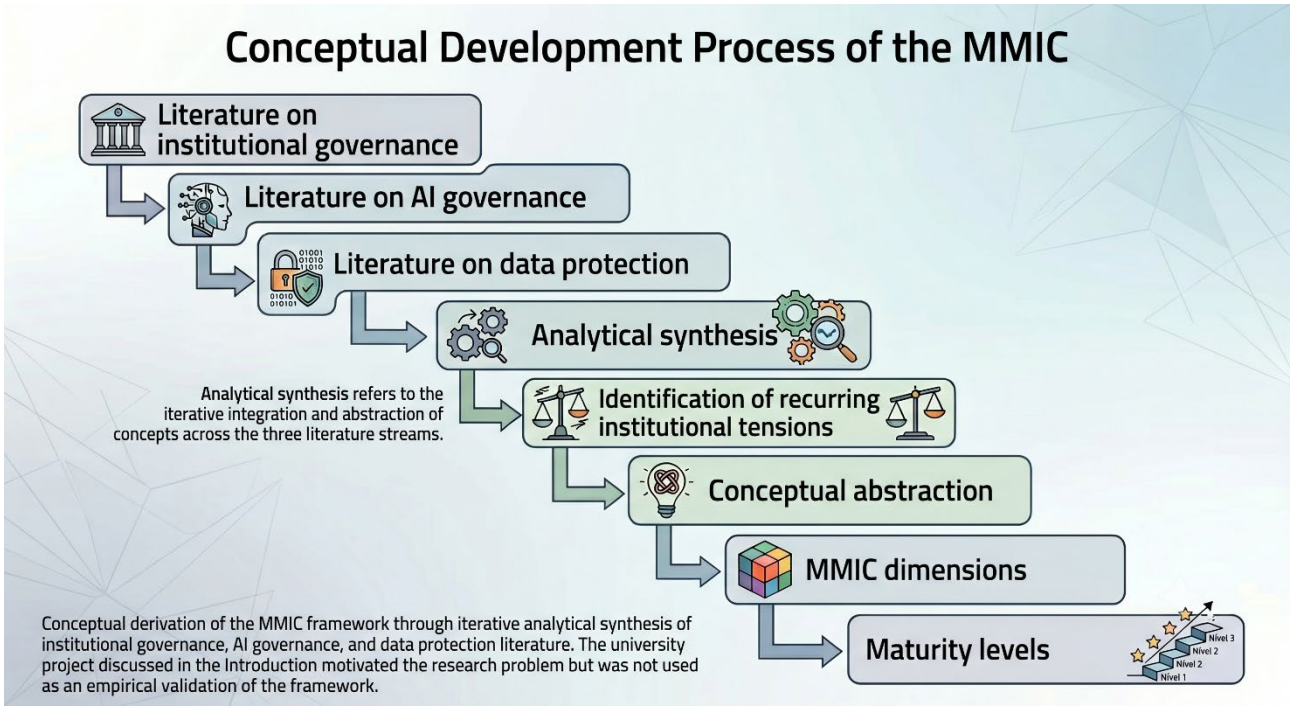


Figure 1. Conceptual development of the MMIC through iterative analytical synthesis of institutional governance, AI governance, and data protection literature. The institutional project described in the Introduction served as the contextual motivation for the research problem.

The conceptual derivation process presented in Figure 1, should therefore, be interpreted as an analytical reconstruction of the framework's theoretical development rather than, as a sequence of empirical research procedures.

1.1. The LGPD and the Principle of Accountability: From Text to Praxis

Article 6, item X, of the LGPD enshrines the principle of responsabilização e prestação de contas ("accountability"), according to which controllers and processors must be able to demonstrate that they have adopted effective measures to ensure compliance with personal data protection rules. As Doneda (2021), observes, this represents an inversion of the traditional logic of compliance: it is not enough to assert conformity; it must be substantiated through documentation, processes, and governance structures.

However, the transposition of this principle into Brazilian institutional reality has proved problematic. A recurring concern in the Brazilian regulatory debate is that organisations, especially in the public sector, may remain at a stage of merely documentary compliance, maintaining formally adequate policies without effective governance structures, training, and incident response mechanisms (ANPD, 2022), a scenario that converges with the phenomenon described here as an institutional consciousness vacuum.

 CC BY-NC 4.0 DEED Attribution-NonCommercial 4.0 International, 2026

It is important to emphasise that the LGPD establishes three central roles in the processing of personal data: controller, processor, and sub-processor (or subcontracted processor). Although doctrine and ANPD guidance describe distinct roles and responsibilities, a governance gap may nonetheless emerge between controller and sub-processor, particularly in complex institutional environments. In such cases the sub-processor may be contracted "on behalf of" the controller without the latter's direct awareness, and without any explicit formal delegation to the processor authorising such an arrangement.

In an institutional AI implementation project at a Brazilian university, this gap became paradigmatically evident. The university acted as the controller, an employee performed the role of processor, and an external generative AI service functioned as a sub-processor for the data being handled. What such a configuration reveals is not a deficiency of any particular institution's compliance structure, but a structural limit common to institutions generally: formal governance frameworks are designed to govern institutional contracting, and therefore lack instruments through which to perceive tool adoption occurring at the individual level. The processing chain extends beyond the perimeter that institutional governance is equipped to observe.

This configuration illustrates that the institutional consciousness vacuum is not limited to cultural or normative spheres but also emerges at the contractual and technological interfaces of the processing chain, where seemingly operational decisions can generate significant legal implications.

From this perspective, the effectiveness of the LGPD does not depend solely on stricter sanctions or more detailed regulations. It requires, above all, the construction of an institutional consciousness capable of recognising data protection as an intrinsic organisational value, not as a merely heteronomous obligation imposed from outside. This transformation, as Bamberger (2010), argues, demands time, committed leadership, and the redesign of institutional incentives.

Within this study, accountability is therefore interpreted, not merely as a legal obligation but as an institutional governance capability whose effectiveness depends upon the degree of institutional consciousness achieved by the organization.

1.1. Artificial Intelligence and the Challenges for Information Governance

The incorporation of artificial intelligence systems into institutional decision-making processes exponentially increases the challenges of data protection. Unlike traditional information systems, in which the processing logic is transparent and auditable, machine learning algorithms, especially those based on deep learning, operate as "black boxes" whose decision-making criteria are not always understandable, even to their own developers (Burrell, 2016).

This algorithmic opacity comes into direct tension with fundamental principles of the LGPD. Article 6, items VI and IX, enshrines the principles of transparency and non-discrimination, ensuring that data subjects have clarity regarding how their data are processed and guaranteeing that they will not be subjected to unlawful discriminatory treatment. In AI systems however, explainability, that is, the ability to express in intelligible language the reasons that led to a given decision, still

 CC BY-NC 4.0 DEED Attribution-NonCommercial 4.0 International, 2026

constitutes a technical challenge that has not been fully resolved. Models based on deep neural networks process millions of parameters whose interactions produce accurate results but opaque justifications.

Information governance in AI environments therefore, cannot be limited to procedural adjustments. It requires, as Janssen and Kuk (2016), argue, an institutional redesign that integrates technical, legal, and ethical competencies into joint deliberative processes. The role of the Data Protection Officer (DPO), provided for in Article 41 of the LGPD, is central in this coordination. However, its effectiveness depends on real institutional empowerment. Where that empowerment is absent, the DPO may be positioned as an isolated advisor, without decision-making authority or adequate resources.

Consequently, AI governance cannot be reduced to technological oversight alone; it necessarily requires institutional structures capable of interpreting, internalising, and operationalising governance principles across organisational decision-making processes.

1.1. Organisational Culture and the Institutionalisation of Norms: Between Ceremonial Isomorphism and Substantive Change

The effective implementation of data protection laws is not merely a technical or legal challenge; it is, above all, a process of cultural transformation. Institutional theory, consolidated in the field of organisational studies, offers useful conceptual tools for understanding why many institutions formally adopt norms without substantively internalising them.

Meyer and Rowan (1977) coined the expression "ceremonial isomorphism" to describe situations in which organisations adopt formal structures with the aim of obtaining external legitimacy, while maintaining internal practices dissociated from those structures. Applied to the LGPD, the concept elucidates a recurring case: institutions that publish detailed privacy policies create data protection committees and appoint DPOs but whose daily routines ignore these mechanisms, treating them as institutional members meant to satisfy audits or avoid penalties.

This decoupling between form and practice does not necessarily stem from organisational errors. Brunsson (2002), argues that in complex organisations the separation between discourse, decision, and action constitutes an adaptive strategy in the face of contradictory pressures. These institutions face simultaneous demands for efficiency, technological innovation, and regulatory compliance, objectives that are at times irreconcilable. As a result, they develop responses that symbolically satisfy each of these demands without fully resolving any of them.

In the Brazilian context, studies on administrative culture (Motta & Alcadipani, 1999; Carvalho & Vieira, 2003), point to persistent traits: formalism (an emphasis on written rules accompanied by weak enforcement), personalism (the prevalence of interpersonal relations over impersonal norms), and aversion to accountability (a structural resistance to rendering accounts). These characteristics help explain why the LGPD, even when formally implemented, faces difficulties in becoming substantively institutionalised.

 CC BY-NC 4.0 DEED Attribution-NonCommercial 4.0 International, 2026

Overcoming this pattern requires an approach that unites normative compliance, ethical reflection, and organisational learning. It is not enough to "comply with" the LGPD; it is necessary to internalise it as part of institutional identity, integrating data protection into strategic decisions, and not only into audit reports.

This perspective reinforces the argument that sustainable governance depends less on formal regulatory adoption than on the institutional internalisation of governance principles.

1.1. Institutional Consciousness: Building an Operational Concept

The expression "institutional consciousness" is used here not as a literary metaphor, but as an operative concept for analysing the degree of reflexivity of an organisation which enables it to see its own practices. The term refers to the capacity to perceive, understand, and adjust the ethical, social, and legal consequences of its actions, especially when they are mediated by technology.

Within organisational theory, this notion approximates what Argyris and Schön (1978) call "double-loop learning": the process by which an institution not only corrects errors within an existing set of rules but also questions the very rules that guide its decisions. In other words, a "conscious" organisation is one that can interrogate its own assumptions—including those that legitimise its operational patterns.

Applied to data protection, institutional consciousness translates into the ability to reflect critically on how and why certain data processing takes place, going beyond formal legal compliance. An institution endowed with such consciousness does not limit itself to avoiding sanctions; it seeks to anticipate risks and ethical dilemmas, recognising that information is sensitive matter involving fundamental rights and therefore, requires continuous governance.

This reflexive dimension approximates the concept of "substantive accountability" (Bovens, 2010), understood not as merely technical reporting, but as the moral and cognitive disposition to respond transparently for the impacts of one's own decisions. From this perspective, institutional consciousness is an emergent attribute of organisational culture, resulting from the interaction between values, practices, and power structures.

One may say, therefore, that the development of institutional consciousness involves three interdependent layers:

1; Normative perception – the recognition of legal and ethical obligations.

2, Organisational reflexivity – the ability to translate these obligations into concrete practices and procedures.

3, Deliberate and continuous action – the disposition to review decisions and adapt behaviour in the face of new technological and social contexts.

These three layers compose a feedback loop in which normative learning generates structural changes, and these reinforce new forms of ethical perception. When the loop is interrupted, whether due to lack of leadership, resources, or institutional clarity, this condition is termed the institutional

 CC BY-NC 4.0 DEED Attribution-NonCommercial 4.0 International, 2026

consciousness vacuum: a condition in which the organisation acts without full understanding of the implications of its actions, even though it possesses formal policies, norms, and compliance structures.

This situation becomes particularly visible in the adoption of AI technologies. In environments where the delegation of decisions to automated systems is rapidly expanding, the absence of institutional consciousness can lead to an uncritical transfer of responsibility from humans to machines. Recent evidence from a survey of knowledge workers indicates that greater reliance on generative AI is associated with reduced cognitive effort and diminished critical engagement with the task at hand (Lee et al., 2025), a dynamic that compounds this transfer of responsibility at the individual level. It is important to emphasise that technology often functions as a mirror: it reflects not only the organisation's operational efficiency, but also the depth — or superficiality — of its ethical consciousness. In most cases, technology simply digitises the business rules that exist (or fail to exist) within the institution, and the absence of such rules becomes more evident and increasingly difficult to manage once technological systems are placed at the forefront.

1.1. Note on the Situated Origin of Research

The initial motivation for the study arises from a concrete experience in which the author took part, in the context of an AI implementation project at a Brazilian university. During the implementation phase, a question raised by a team member regarding the system's compliance with the LGPD made visible a difficulty that formal governance frameworks share generally: assessing, in advance, the data-protection implications of AI tools adopted at the individual level (von Garrel & Mayer, 2025).

The subsequent development of the research relied on a literature review, analysis of publicly available regulatory instruments and theoretical construction, as detailed in the previous subsections. This methodological choice avoids reporting institution-specific data and does not identify the programs or individuals involved, while simultaneously enabling theoretical generalisation applicable to a variety of organisational contexts.

The Institutional Consciousness Vacuum in the Application of the LGPD to AI Systems

The advancement of AI in institutional environments, challenges, not only technological infrastructure, but also the ethical and legal consciousness of organisations. When the use of technology precedes an understanding of its impacts, a zone of indetermination emerges; a space in which responsibilities become diluted, and decisions are made without clarity about their consequences. It is within this interstice that the institutional consciousness vacuum takes shape. This problem becomes even more acute when individuals begin to delegate to technology, particularly AI, responsibilities that should remain their own, a shift that raises significant ethical and technical concerns.

 CC BY-NC 4.0 DEED Attribution-NonCommercial 4.0 International, 2026

This vacuum does not appear abruptly. It is consolidated gradually, as the discourse of innovation overrides ethical reflection and the imperative of technical efficiency displaces substantive responsibility. The promise of automation, speed, and cost reduction tends to eclipse the debate on risks, rights, and duties. The result is a culture of blind delegation, in which technology is endowed with an aura of neutrality that it, in fact, does not possess.

The condition this study seeks to characterise, is one in which institutions, whether public or private, implement AI systems without prior mapping of data processing operations, without impact assessments, and without a clear definition of the agents involved. In such a configuration, the technical operator may assume a decision-making role that exceeds their formal competence: subcontracting tools, adjusting data flows, and defining model training parameters without explicit authorisation from the controller. The normative gap between controller, processor, and sub-processor appears here in its most critical form: implicit delegation without explicit responsibility.

The data-protection implications of large language models depend less on the model than on its deployment architecture. Proprietary, cloud-hosted models accessed as external services (such as ChatGPT) necessarily transfer data beyond the institutional boundary, inserting the provider into the processing chain as a processor or sub-processor and making the controller dependent on the provider's contractual and jurisdictional guarantees. Self-hostable, open-weight models can instead be deployed within the institution's own infrastructure, keeping personal data inside the controller's boundary and removing the external sub-processor from the chain. This is not a claim that any particular model is 'compliant' in the abstract — compliance is a property of institutional arrangement, not of the software — but the choice of deployment architecture directly determines which LGPD obligations are triggered, and which actors enter the accountability chain. Within the MMIC, the capacity to recognise and deliberate on this choice ex ante is itself a marker of institutional consciousness: an Unconscious institution adopts whichever tool is most convenient without registering the data-flow implications, whereas an integrated institution treats deployment architecture as a governance decision taken before adoption.

From a legal standpoint, the vacuum manifests as misalignment between formal responsibility and actual responsibility. While the LGPD distributes obligations precisely, institutional practice often reallocates technical execution to intermediate levels of the hierarchy without the necessary contractual or procedural support. The risk is not only noncompliance with the law, but also erosion of accountability; a systemic weakening of the institution’s capacity to answer for its actions and to demonstrate regulatory good faith.

From an epistemological standpoint, this is a case of cognitive disconnection: the institution acts but does not fully understand the scope of its actions. There are processes, but no meaning, norms, but no internalisation. This disconnection is a symptom of hypertrophied instrumental rationality, typical of contexts in which technology is seen as a self-sufficient solution. The technical apparatus paradoxically becomes an instrument of institutional alienation, the more processes are automated, the weaker the perception of their human and ethical impacts.

 CC BY-NC 4.0 DEED Attribution-NonCommercial 4.0 International, 2026

Authors such as Zuboff (2019), and Eubanks (2018), warn of the tendency for "algorithmic governments and corporations" to replace human judgment with computational metrics, diluting responsibility in complex networks of automated decision-making. When this occurs within public institutions, the problem acquires a democratic dimension: decisions that affect fundamental rights come to be mediated by systems whose internal logic escapes social control.

In this sense, the institutional consciousness vacuum can be understood as the absence of systemic reflexivity. It is not simply a matter of negligence or omission, but a structural inability to question operational assumptions. The institution becomes efficient at performing routines, yet blind to the moral implications of its own efficiency.

Overcoming this vacuum requires more than new regulations. It demands cognitive and ethical infrastructures: multidisciplinary teams, technological ethics committees, independent algorithmic audits, and continuous training programs. Such mechanisms should operate not as punitive control bodies, but as spaces for institutionalised reflection, capable of reintroducing critical thinking into the decision-making cycle.

The objective is not to slow down innovation: to place the human back at the centre of the relationship between data, algorithms, and decisions. An institution endowed with consciousness is not one that avoids error altogether, but one that learns from its errors, revisits its choices, and recognises the moral complexity of automating the world.

Accordingly, the institutional consciousness vacuum should be interpreted as an analytical condition preceding observable governance failures, rather than as a consequence of regulatory noncompliance itself.

1.1. Conceptualisation and Delimitation of the Phenomenon

The institutional consciousness vacuum is an organisational phenomenon characterised by the absence of alignment between formal compliance with data protection rules and an effective awareness of the ethical, legal, and informational obligations involved in the processing of personal data, particularly in contexts that employ AI systems.

This definition deliberately distinguishes the institutional consciousness vacuum from isolated operational failures, emphasising its systemic and institutional nature, rather than individual procedural deficiencies.

It is a gap that cannot be reduced to legal noncompliance situations, in which the organisation simply violates the law out of negligence or bad faith. The vacuum is more subtle and, for that very reason, more insidious: it manifests in organisations that, formally, meet the basic requirements of the LGPD (they have a privacy policy, have appointed a Data Protection Officer, have produced documentation), but lack structures, processes and, above all, a culture capable of operationalising these mechanisms in a substantive way.

This mismatch generates a gray zone in which critical decisions (such as implementing new AI systems, defining processing purposes, or choosing legal bases) are taken without clarity regarding

 CC BY-NC 4.0 DEED Attribution-NonCommercial 4.0 International, 2026

institutional roles, without adequate risk assessment, and without effective accountability mechanisms. Responsibility, which legally belongs to the controller (the institution), is in practice, diluted among multiple actors (technicians, managers, legal advisors) who operate in a fragmented way, often unaware of or underestimating the implications of their choices.

It is useful to distinguish the institutional consciousness vacuum from related concepts. It differs from "lack of compliance" because it can coexist with formal LGPD adaptation programs. It differs from "institutional bad faith" because it does not presuppose deliberate intent to violate rights. It also differs from "technical incompetence," as it cannot be reduced to a lack of specialised knowledge in data protection or AI. The vacuum is, fundamentally, a deficit of information governance and organisational culture gap that no isolated hiring of experts or adoption of security technologies can, by itself, fill.

1.1. Symptomatology: Typical Manifestations of the Vacuum

The institutional consciousness vacuum manifests through observable signs that, although varying by context, display recurring patterns. The following symptoms should not be interpreted as isolated organisational deficiencies but as interconnected manifestations of the same institutional governance condition. Four main symptoms can be identified:

Symptom 1, Fragmented Decision-Making

There is a lack of integration between legal, technical, and administrative areas in decision-making processes involving data processing. Where this integration is absent, decisions about the implementation of AI systems may be made by information technology departments without prior consultation with legal teams or the Data Protection Officer. Conversely, legal departments draft privacy policies without sufficient technical understanding of how the systems operate. In the most complex situations, internal disparities and conflicts further intensify the difficulty of mitigating these gaps. This fragmentation produces a paradoxical effect: multiple areas assume that "another area" is responsible for LGPD compliance. Technicians presume that legal counsel has validated legality; legal teams presume that technicians have implemented the appropriate safeguards; managers presume that both have addressed the issue. The result is a void of actual responsibility, in which everyone—and simultaneously no one—considers themselves accountable.

Regulatory guidance and organisational studies have repeatedly noted that data protection officers are frequently excluded from decisions on the adoption of automated systems (EDPB, 2022). In the Brazilian context, although systematic data are lacking, anecdotal evidence and reports from DPOs suggest an even more fragmented reality, given the lower level of institutional maturity in data governance.

Symptom 2, Informal Delegation of Responsibilities

The vacuum often produces an overload on individuals or small technical teams that, in the absence of formal governance structures, informally assume responsibility for LGPD compliance. These actors often operate without a clear mandate, without adequate resources and, crucially, without institutional decision-making power.

 CC BY-NC 4.0 DEED Attribution-NonCommercial 4.0 International, 2026

An unsustainable situation emerges: legal responsibilities that belong to the institution as controller are, in practice, exercised by individuals who lack the authority to implement structural changes. Where this misalignment occurs, technical staff may identify risks and produce recommendations without holding the authority to implement the structural changes those recommendations require. The gap is structural rather than attributable to any particular actor: it reflects how formal responsibility and operational capacity are distributed across governance layers.

This informal delegation also generates a risk of personal liability. Article 42 of the LGPD establishes joint liability of controller and processor for damage caused; although the law does not criminally punish individuals for violations (except in specific cases), administrative proceedings and civil actions may attempt to identify direct responsible parties. Professionals operating within the vacuum thus become exposed to risks disproportionate to their institutional position and decision-making capacity.

Symptom 3, Reactive Culture

Organisations immersed in the institutional consciousness vacuum tend to act exclusively in a reactive manner: they move only in the face of security incidents, data subject complaints, ANPD notifications, or negative media coverage. They do not develop proactive capacities for risk management, impact assessment, or continuous monitoring.

This reactive posture stands in stark contrast to the principle of accountability, which demands continuous demonstration of compliance. Reactive organisations produce documentation post factum, justify decisions retroactively, and implement emergency corrective measures. They lack mechanisms for prevention, internal auditing, or systematic organisational learning.

The reactive culture ultimately reveals that data protection is not perceived as an institutional value, but as a risk to be minimally managed. Compliance becomes an exercise in damage control, not in building sustainable ethical practices. Such a posture is particularly problematic in AI contexts, where design decisions taken in the early stages of development have long-lasting and difficult-to-reverse consequences.

Symptom 4, Ethical Invisibility

Perhaps the deepest symptom of the vacuum is the absence of institutional debate on the ethical and epistemological dimensions of the AI systems implemented. Discussions focus on technical aspects (accuracy, performance, computational efficiency) and legal aspects (formal compliance with legislation), but rarely address questions, such as: What values are embedded in the algorithms?, What worldviews are reflected in the training data?, Which social groups may be harmed by algorithmic biases?, How can we ensure that automated systems do not reproduce historical discrimination?

This ethical invisibility is particularly serious in the public sector, where AI systems can directly impact citizens' fundamental rights, for example, determining who accesses social benefits, who is subjected to police investigations, or who receives priority in medical service queues. Algorithmic

 CC BY-NC 4.0 DEED Attribution-NonCommercial 4.0 International, 2026

decisions that affect human lives are frequently treated as neutral technical choices, devoid of value-laden content.

The absence of AI ethics committees, public consultations on system implementation, or institutional channels in which social impacts can be debated, reveals that the ethical dimension remains off the institutional radar. The organisation operates technologically but does not ethically reflect on its technological choices.

1.1. Typology of the Vacuum: Modalities and Contexts

Although the institutional consciousness vacuum displays common characteristics, it manifests in different ways depending on the organisational context.

The proposed typology reflects analytically distinguishable manifestations of the institutional consciousness vacuum. Although presented separately for explanatory purposes, these modalities frequently coexist and reinforce one another within organisational contexts.

A preliminary typology is proposed here, identifying four main modalities:

1, Structural Vacuum

This is characterised by the complete absence of formal data governance structures. The institution lacks committees, clearly defined policies, documented procedures, or designated decision-making bodies. Where a DPO exists, they operate in isolation, without institutional support. Decisions regarding data processing occur on an ad hoc basis, without consistent criteria.

This modality is typical of organisations at an early stage of maturity that have not yet understood the need to structure information governance processes. It is prevalent in small institutions, with limited resources and low technical capacity, but, surprisingly, it can also be found in large and complex organisations where data protection has never been prioritised strategically.

2, Cultural Vacuum

This occurs when formal structures exist but are not internalised by organisational culture. There is a privacy policy, appointed committees, documented procedures, but such mechanisms remain dead letter, ignored in everyday practices. Staff members are unaware of or disregard guidelines, managers prioritise other objectives, and senior leadership does not demonstrate genuine commitment.

This modality exemplifies the "ceremonial isomorphism" discussed earlier: the organisation adopts external forms of compliance without substantive transformation. The cultural vacuum is especially resistant, because structural changes prove insufficient; transformation of mindsets, values, and practices is required, and this is a slow and complex process.

3, Technical Vacuum

 CC BY-NC 4.0 DEED Attribution-NonCommercial 4.0 International, 2026

This manifests when there is institutional intent to comply, but a lack of technical competencies prevents adequate operationalisation. The organisation recognises the importance of data protection, establishes guidelines, but lacks skilled professionals to implement safeguards, conduct DPIAs, audit algorithms, or respond adequately to incidents.

This type of vacuum is particularly common in institutions facing budget constraints, difficulties in hiring qualified specialists, or limitations imposed by civil service regimes. It differs from the previous modalities because it does not arise from disinterest or cultural resistance, but from objective capacity constraints.

4, Political Vacuum

This is characterised by the lack of strategic prioritisation of data protection by the institution's senior leadership. Although structures, a favourable culture, and technical competencies may exist at operational levels, the absence of political support from top management, and from key stakeholders themselves, prevents data governance from becoming effectively institutionalised. Resources are not allocated, technical recommendations are disregarded, and conflicts between operational efficiency and compliance are systematically resolved in favour of the former.

This vacuum reveals that data protection, despite being a legal requirement, is not part of the institutional strategic core. It remains at the periphery of top management's concerns, mobilised only when reputational risks or sanctions become imminent.

1.1. Consequences of the Vacuum: Systemic Risks

The institutional consciousness vacuum is not merely an academic phenomenon; it produces concrete consequences across multiple dimensions:

Legal Risks: The LGPD establishes administrative sanctions that may reach, at the limit, 2% of the organisation's revenue (art. 52, II), capped at 50 million reais per infraction. Although the ANPD has so far adopted a pedagogical stance, with gradual application of penalties, the maturation of the regulatory system tends to tighten enforcement. Organisations immersed in the vacuum are in a situation of heightened legal vulnerability.

Operational Risks: Security incidents, data breaches, and inappropriate use of AI systems can lead to operational disruptions, loss of critical data, and the need for costly emergency corrective measures. The absence of structured risk management processes amplifies both the likelihood and the impact of such events.

Reputational Risks: In a society increasingly attuned to issues of privacy and ethical use of AI, violations or inappropriate use of personal data generate immediate negative repercussions, with the potential to cause lasting damage to institutional image. For public organisations, this can translate into loss of citizen trust, for private organisations, into loss of market share.

 CC BY-NC 4.0 DEED Attribution-NonCommercial 4.0 International, 2026

Risks to Data Subjects: The most serious consequence, and often rendered invisible, is that the institutional vacuum exposes data subjects to violations of fundamental rights. AI systems implemented without adequate governance can produce discriminatory decisions, violate privacy, and cause material and moral harm to individuals who had no participation in the institutional choices that affect them.

These consequences therefore, reinforce the central proposition of this study: governance failures frequently originate from institutional deficiencies preceding observable regulatory non-compliance.

1.1. Positioning Institutional Consciousness

The concept of Institutional Consciousness, proposed in this study, shares certain characteristics with existing constructs frequently employed in governance and organisational studies. Nevertheless, it represents a distinct analytical perspective. Rather than measuring organisational performance, governance effectiveness, or ethical culture independently, Institutional Consciousness seeks to explain the institutional capacity to recognise, internalise, and operationalise governance principles before compliance failures become observable.

Several related constructs have contributed significantly to understanding organisational governance. Organisational maturity models generally assess the evolution of organisational capabilities, processes, or digital transformation. Governance capability, focuses primarily on the existence and effectiveness of governance structures, decision-making arrangements, and organisational competencies. Ethical climate emphasises shared organisational values and behavioural norms influencing ethical decision-making. Institutional reflexivity, in turn, highlights the capacity of institutions to critically evaluate their own practices and adapt to changing societal and regulatory conditions.

Although these constructs provide valuable analytical lenses, none explicitly addresses the institutional conditions through which governance principles become cognitively embedded and operationalised across organisational structures prior to the emergence of regulatory failures. Institutional Consciousness therefore occupies a complementary, rather than competing position within the governance literature.

Table 1. Conceptual positioning of Institutional Consciousness

Construct	Primary focus	Analytical emphasis	Distinction from MMIC
Organisational maturity	Evolution of organisational capabilities	Performance and capability development	MMIC evaluates institutional awareness preceding capability development
Governance capability	Governance structures and decision-making	Institutional governance effectiveness	MMIC emphasises institutional recognition and internalisation of governance principles
Ethical climate	Shared organisational values	Ethical behaviour and organisational culture	MMIC focuses on governance preparedness

 CC BY-NC 4.0 DEED Attribution-NonCommercial 4.0 International, 2026

			rather than ethical culture alone
Institutional reflexivity	Institutional learning and adaptation	Reflective institutional change	MMIC operationalises institutional awareness through structured maturity levels
Institutional Consciousness (MMIC)	Institutional awareness of governance implications	Translation of governance principles into institutional practice	Integrates governance, AI governance, and data protection into a unified conceptual framework

Institutional Consciousness should, therefore, be understood as an antecedent governance condition, rather than as an indicator of organisational success or regulatory compliance. Organisations may formally comply with legal requirements while simultaneously exhibiting low levels of institutional consciousness if governance principles remain fragmented, weakly internalised, or disconnected from everyday decision-making processes. Conversely, institutions demonstrating higher levels of institutional consciousness are expected to anticipate governance challenges proactively, integrate legal and ethical principles into organisational routines, and develop governance capabilities that extend beyond minimum regulatory compliance.

From this perspective, the MMIC does not replace existing governance or maturity models. Instead, it complements them by introducing an institutional-level analytical construct specifically designed to explain why formally compliant organisations may still experience governance failures during AI adoption. The framework, therefore, contributes a conceptual bridge between institutional governance theory, AI governance, and data protection literature, offering a structured basis for future empirical operationalisation and comparative institutional analysis.

Institutional Consciousness Maturity Model

The Institutional Consciousness Maturity Model (MMIC) shouldtherefore be understood as an analytical governance framework rather than a regulatory compliance checklist. Accordingly, the MMIC operationalises Institutional Consciousness by translating an abstract theoretical construct into an analytical governance framework capable of supporting institutional diagnosis and future empirical assessment.

The need for diagnostic instruments capable of assessing the degree of institutional consciousness in matters of data protection motivated the development of the MMIC. This model proposes a lens for observation and continuous improvement for organisations that seek to integrate information governance, technological ethics, and legal compliance in environments mediated by AI.

 CC BY-NC 4.0 DEED Attribution-NonCommercial 4.0 International, 2026

The conception of the MMIC starts from the premise that institutional maturity is not limited to the existence of formal policies and procedures, but involves the capacity to reflect, learn, and adapt in the face of new normative and technological contexts. Thus, the model articulates technical, normative, and cultural dimensions in a progressive framework that enables organisations to identify their current stage and define strategies to evolve toward integrated institutional consciousness.

To situate the proposed model within the international ecosystem of AI governance, the diagram below illustrates the interdependence between data protection regulatory frameworks and management systems based on international standards:

Figure 2: Privacy-Infused AI Governance
(Source: Author's elaboration adapted from ISO/IEC 42001 frameworks and data protection laws – LGPD, GDPR, and PDPL.)

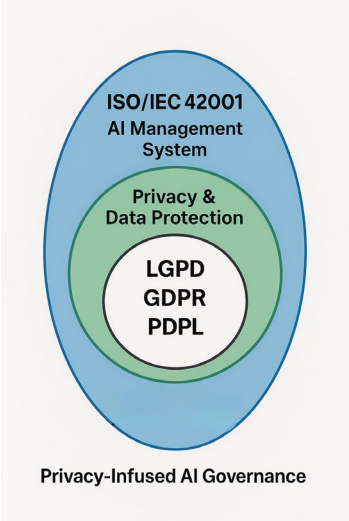


Figure description:

The diagram highlights the layered structure of AI governance permeated by privacy (privacy-infused governance). At the core lie data protection laws (LGPD, GDPR, PDPL), which constitute the legal foundation. Surrounding them are privacy and data protection practices, which function as the operational layer that applies legal principles. The third layer represents the AI Management System, based on ISO/IEC 42001, which incorporates control policies, risk mitigation, and continuous auditing. Encompassing all layers is the concept of Privacy-Infused AI Governance, which expresses the ethical, technical, and normative integration of privacy, transparency, and accountability.

This structure shows that AI governance anchored in privacy must be built from the inside out: one starts from normative compliance (the legal core), expands to the operationalisation of data protection controls, and culminates in the strategic and cultural management of artificial intelligence.

 CC BY-NC 4.0 DEED Attribution-NonCommercial 4.0 International, 2026

1.1. Foundations of the Model

The analytical dimensions proposed by the MMIC were not predefined organisational categories. They emerged through iterative analytical abstraction of recurring governance tensions repeatedly identified across the three literature domains. Each dimension, therefore, represents a distinct manifestation of institutional consciousness rather than an independent organisational capability or regulatory requirement.

The MMIC is based on the integration of four conceptual pillars:

1, Accountability and Responsibility: the duty to demonstrate compliance and transparency in data processing practices.

2, Institutional Reflexivity: the capacity for learning and adaptation in the face of normative and technological changes.

3, Ethical Organisational Culture: the incorporation of data protection as an organisational value.

4, AI Governance: the management of risks and impacts resulting from automated decisions.

Inspired by frameworks, such as CMMI (Capability Maturity Model Integration) and COBIT (Control Objectives for Information and Related Technologies), the model proposes a path of progressive development in which the institution moves from a stage of formal obedience to a state of full integration between ethical values, technical practices, and control mechanisms.

1.1. Maturity Levels of Institutional Consciousness

The maturity levels should not be interpreted as fixed organisational categories but as progressive analytical stages describing increasing degrees of institutional awareness regarding AI governance and data protection. The MMIC is structured into four gradual levels of development:

Level 1 : Unconscious

The institution is unaware of LGPD obligations, has no internal privacy policies, and lacks control mechanisms. Decisions are fragmented and reactive, based on improvisation and ad hoc responses to incidents.

Level 2,:Reactive

There is awareness of the legislation, but actions are driven by external demands or crises. The focus falls on the minimum fulfillment of legal obligations, without integration between technical and administrative areas.

Level 3: Conscious

The organization implements a formal governance structure, appoints DPOs, defines processing flows, and promotes training. A culture of compliance begins to emerge and expand, although it still depends heavily on individual leadership.

 CC BY-NC 4.0 DEED Attribution-NonCommercial 4.0 International, 2026

Level 4 : Integrated

Data protection becomes part of the institutional identity. AI management incorporates privacy by design and ethics by default practices. The institution adopts internal audits, continuously reviews its processes, and exercises ethical leadership in the digital ecosystem.

The maturity levels should be interpreted as progressive degrees of institutional awareness concerning AI governance and data protection, rather than measures of organisational performance or regulatory success. They describe the gradual institutionalisation of governance principles across organisational structures, decision-making processes, and operational practices.

1.1. Analytical Dimensions of the Model

Each analytical dimension represents a recurrent governance tension identified during the analytical synthesis process rather than an isolated organisational capability or regulatory requirement. Each level is analysed through four interdependent dimensions:

1, Cognitive: the degree of organisational awareness regarding risks and ethical principles.

2, Normative: legal and documentary adequacy to the LGPD regime.

3, Pragmatic: operationalisation of controls, audits, and incident responses.

4, Reflexive: capacity for self-assessment and continuous institutional learning.

These dimensions are not static but dynamic: progress in one reinforces the others, generating virtuous cycles of maturity. Institutional diagnosis should therefore be understood as an iterative process rather than as a one-off audit.

1.1. Internal Architecture and Correspondence of the Components

To clarify the internal architecture of the MMIC, its components are distinguished by analytical function rather than treated as parallel lists. The four conceptual pillars (Accountability and Responsibility, Institutional Reflexivity, Ethical Organisational Culture, and AI Governance) are the theoretical foundations from which the construct is built. The four analytical dimensions (Cognitive, Normative, Pragmatic, and Reflexive) are the axes along which institutional consciousness is assessed. The four maturity levels describe the progressive degree to which governance principles become institutionalised along those axes. Finally, the symptoms and the typology of the institutional consciousness vacuum, introduced in Section 4, operate as diagnostic signatures — observable indications of where an institution is likely to sit on the maturity scale. Table 2, makes these correspondences explicit.

Table 2. Correspondence between diagnostic signatures and the MMIC's analytical dimensions, indicative maturity levels, and conceptual pillars

Diagnostic signature	Primary dimension(s)	Indicative maturity level	Related pillar

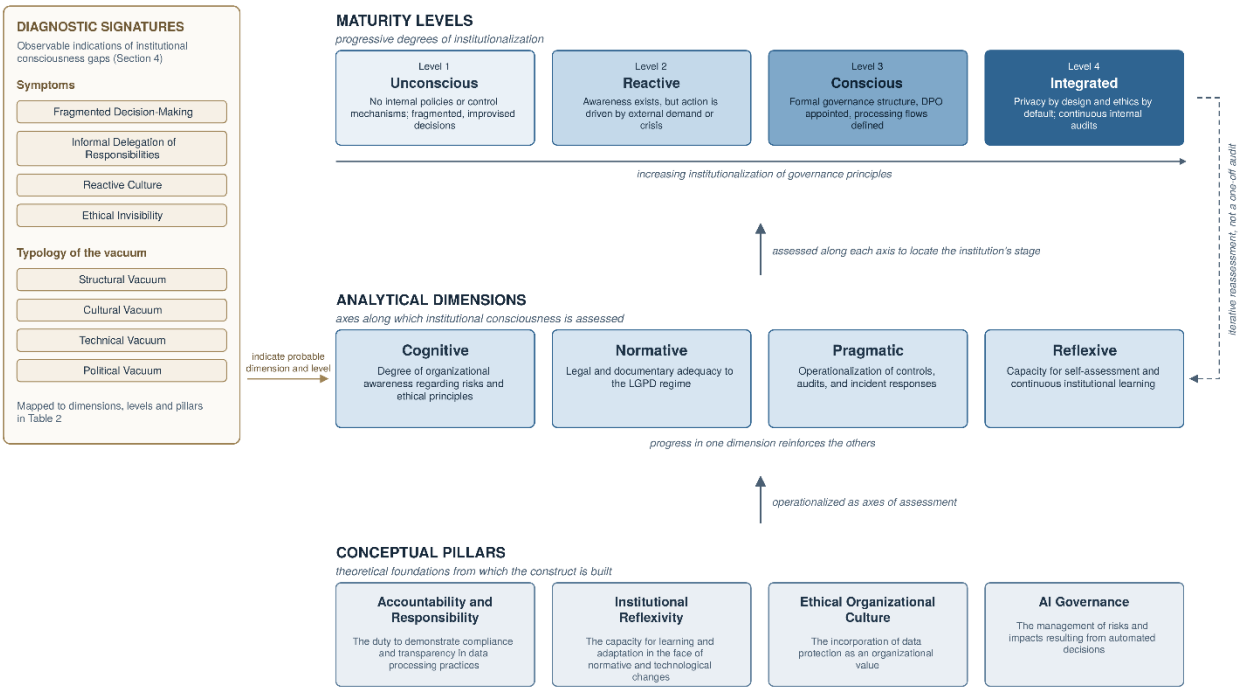
 CC BY-NC 4.0 DEED Attribution-NonCommercial 4.0 International, 2026

Fragmented Decision-Making	Pragmatic, Normative	1–2	Accountability; AI Governance
Informal Delegation	Normative, Pragmatic	1–2	Accountability
Reactive Culture	Reflexive	2	Institutional Reflexivity
Ethical Invisibility	Cognitive, Reflexive	1	Ethical Organisational Culture
Structural Vacuum	Normative, Pragmatic	1	(governance structures absent)
Cultural Vacuum	Reflexive, Cognitive	2–3	Ethical Organisational Culture
Technical Vacuum	Pragmatic	cross-level	AI Governance
Political Vacuum	Normative (strategic)	cross-level	Accountability

To illustrate how these components operate together, consider a configuration in which an AI tool is adopted on behalf of a controller without a formal delegation instrument. This pattern exemplifies the symptom of Fragmented Decision-Making and a Structural Vacuum, located on the Normative and Pragmatic dimensions. Where the assumption prevails that publicly available data fall outside the scope of protection, the pattern also exemplifies Ethical Invisibility on the Cognitive dimension. Configurations of this kind correspond to the conditions the lowest maturity levels are intended to capture.

Figure 3. Architecture of the MMIC. The conceptual pillars provide the theoretical foundations from which the construct is built; the analytical dimensions constitute the axes along which institutional consciousness is assessed; and the maturity levels describe progressive degrees of institutionalation. Diagnostic signatures — the symptoms and the typology of the institutional consciousness vacuum discussed in Section 4 — indicate the probable dimension and maturity level, as detailed in Table 2. The dashed return path represents the iterative character of institutional diagnosis. (Source: Author's elaboration.)

 CC BY-NC 4.0 DEED Attribution-NonCommercial 4.0 International, 2026



1.1. Applicability and Operationalization

The MMIC can be used in four main contexts:

1, Institutional self-diagnosis – identification of the current maturity stage and governance gaps.

2, Strategic planning – definition of compliance goals and investment priorities.

3, Organisational benchmarking – comparison between units or similar institutions.

4, Institutional communication – public demonstration of commitment to ethics and data protection.

Applying the model requires the development of a validated measurement instrument composed of qualitative and quantitative indicators distributed across the four dimensions. The empirical validation of the MMIC should be carried out in future research to consolidate its theoretical robustness and practical applicability.

The MMIC is intentionally designed to facilitate future empirical operationalisation. Its analytical dimensions may be translated into qualitative assessment protocols, organisational self-assessment instruments, or quantitative maturity indicators in subsequent research.

The MMIC applies to both public and private institutions, but the two contexts shape how it is read. In the public sector, institutional consciousness gaps intersect with constitutional duties, democratic accountability, and citizens' inability to opt out of automated decisions; the framework's diagnostic value lies in exposing where formal compliance coexists with weak democratic safeguards.

 CC BY-NC 4.0 DEED Attribution-NonCommercial 4.0 International, 2026

In the private sector, the same gaps surface at the intersection of commercial incentives, reputational exposure, and contractual processing chains; its value lies in revealing where efficiency pressures override substantive protection. The dimensions and maturity levels are common to both, but the consequences of a low-consciousness state — and therefore the management implications of advancing along the scale — are weighted differently: democratic legitimacy and rights protection in the public sector, market trust and liability exposure in the private. This also bounds the framework's generalisability: the MMIC characterises an institutional condition that recurs across sectors, while the specific drivers and stakes remain sector-dependent.

1.1. Considerations on Implementation and Ethical Governance

Institutional maturity, in the context of the LGPD and AI, is not an endpoint but a process of continuous evolution. Consolidating the MMIC requires political engagement, technical capacity-building, and leadership committed to ethical values.

More than a compliance instrument, the model proposes a pact for organisational learning: that institutions recognise their vulnerabilities, reflect on their decisions, and incorporate ethics of responsibility at all levels of management.

The framework encourages institutions to move beyond regulatory conformity towards governance cultures capable of anticipating emerging ethical and organisational challenges associated with AI.

The MMIC, therefore, provides an analytical bridge through which institutional consciousness may be systematically examined, diagnosed, and progressively strengthened across different organisational contexts.

Discussion

The principal contribution of this study lies not in proposing an additional governance maturity model, but in repositioning institutional preparedness as an antecedent condition for effective AI governance and substantive data protection compliance.

There is an uncomfortable observation that served as the starting point for this study: in many institutions, the LGPD is applied with technical rigour but with little awareness of the meaning behind each action. What is prescribed by the regulation is fulfilled, yet the understanding of why it is done dissipates along the way. It is a form of formal adherence—coherent on paper, but fragile in substance.

The proposed MMIC is compatible with recent developments in AI governance that increasingly advocate governance systems integrating legal, organisational, ethical, and technical dimensions. Rather than functioning as an alternative governance framework, the MMIC offers an institutional diagnostic perspective capable of complementing emerging governance standards by focusing on the organisational conditions necessary for their effective implementation.

 CC BY-NC 4.0 DEED Attribution-NonCommercial 4.0 International, 2026

Rather than introducing another governance instrument, the MMIC provides an analytical lens through which institutions may identify governance deficiencies before they materialise as observable compliance failures.

From a theoretical perspective, the MMIC contributes by integrating institutional governance, AI governance, and data protection into a single analytical framework. Rather than treating these domains as parallel discussions, the model explains how their convergence reveals institutional conditions that frequently remain invisible when each literature is considered independently.

In public bodies, the model can strengthen coherence between discourse and practice, bringing transparency and trust closer together. In the private sector, it serves as an ethical reference, helping transform expressions, such as privacy by design and ethics by default into concrete attitudes embedded in daily project routines. It is less about following a protocol and more about sustaining commitment.

From a practical perspective, the MMIC provides organisations with an analytical instrument for diagnosing institutional preparedness prior to AI deployment. Rather than replacing existing governance standards, the framework complements them by focusing on the organisational conditions necessary for their effective implementation across different institutional settings.

The international dialogue reinforces the meaning of this proposal. The LGPD, GDPR, and PDPL share the same ethical foundation: active responsibility. What varies is how each society translates that idea into practice. The MMIC situates itself in this landscape as a Brazilian contribution, grounded in implementation experiences and the concrete dilemmas that accompany regulatory compliance.

ISO/IEC 42001 and the OECD Principles on AI also move in this direction by integrating ethics and governance. The MMIC adds a dimension that these frameworks sometimes overlook: the cultural one. Without organisational culture, governance norms risk becoming procedural routines; when internalised institutionally, they become sustainable governance practices.

Even so, the model has limits. For now, it is theoretical. It must still be tested in real-world contexts and confronted with the unpredictability of practice. This is its main limitation. The other is the interdisciplinary challenge: dialogue between law, engineering, and management is still the exception rather than the rule.

Although the MMIC remains a conceptually derived framework, the propositions advanced in this study are sufficiently explicit to support future empirical operationalisation and comparative institutional analysis. These observations provide the basis for concluding reflections regarding the theoretical implications, practical limitations, and future empirical development of the MMIC.

Conclusions and Recommendations

This study concludes that effective implementation of the LGPD depends not only on legal and technical compliance but also on the institutional capacity to internalise governance principles. From

 CC BY-NC 4.0 DEED Attribution-NonCommercial 4.0 International, 2026

this perspective, the MMIC provides a theoretically grounded analytical framework through which institutional preparedness for AI governance may be systematically examined.

Institutions evolve through continuous processes of learning, adaptation, and reinterpretation. It is precisely within this movement that learning becomes consolidated and turns into conviction.

The recommendations that follow do not close the debate. They simply broaden the field of action.

The following recommendations derive directly from the theoretical implications of the MMIC and are intended to support institutional learning rather than prescribe universal governance solutions.

For Public and Private Institutions:

- Use the MMIC as a tool for self-knowledge, not as an audit mechanism.
- Value the DPO as a mediator between domains, not as a bureaucratic link.
- Transform formal training sessions into spaces for conversation and experiential exchange.
- Embed privacy by design and ethics by default at the beginning of projects, not at the end, when it is often too late to correct the underlying intent.

For the ANPD:

- Support programs for progressive institutional maturation.
- Produce sector-specific guidelines, with attention to the ethical governance of artificial intelligence.
- Encourage practices that nurture institutional consciousness, beyond mere documentary evidence of compliance.

For Researchers and Policymakers:

- Test the model empirically across diverse contexts and examine how it interacts with public trust.
- Investigate the relationship between institutional maturity and the effectiveness of the LGPD.
- Connect this discussion to international debates on responsible AI and data ethics, while preserving a local, realistic perspective.

Ultimately, the principal contribution of this study lies in proposing Institutional Consciousness as an analytical governance construct capable of complementing existing AI governance and data protection frameworks. Future empirical research will determine the extent to which the MMIC can

 CC BY-NC 4.0 DEED Attribution-NonCommercial 4.0 International, 2026

be operationalised across different institutional contexts, refined through practical application, and incorporated into broader discussions concerning responsible AI governance.

This study is limited by its conceptual nature and does not provide empirical validation of the MMIC. Although the proposed framework was systematically derived through analytical synthesis of the literature, its practical applicability, measurement properties, and predictive capacity remain subjects for future empirical investigation. Future empirical research will determine the extent to which the MMIC can be operationalised across different institutional contexts, refined through practical application, and incorporated into broader discussions concerning responsible AI governance.

References

Argyris, C., & Schön, D. A. (1978). Organizational learning: A theory of action perspective. Addison-Wesley.

Autoridade Nacional de Proteção de Dados. (2022). Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado (Versão 2.0). ANPD. https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf

Bamberger, K. A. (2010). Technologies of compliance: Risk and regulation in a digital age. Texas Law Review, 88(4), 669–739. https://ssrn.com/abstract=1463727

Bovens, M. (2010). Two concepts of accountability: Accountability as a virtue and as a mechanism. West European Politics, 33(5), 946–967.

Brasil. (2018). Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União. http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

Brunsson, N. (2002). The organization of hypocrisy: Talk, decisions and actions in organizations (2nd ed.). Copenhagen Business School Press.

Burrell, J. (2016). How the machine “thinks”: Understanding opacity in machine learning algorithms. Big Data & Society, 3(1), 1–12. https://doi.org/10.1177/2053951715622512

Carvalho, C. A. P. de, & Vieira, M. M. F. (Orgs.). (2003). Organizações, cultura e desenvolvimento local: A agenda de pesquisa do Observatório da Realidade Organizacional. Editora Universitária UFPE.

Choo, C. W. (2003). A organização do conhecimento: Como as organizações usam a informação para criar significado, construir conhecimento e tomar decisões. Senac.

Davenport, T. H. (1998). Ecologia da informação: Por que só a tecnologia não basta para o sucesso na era da informação. Futura.

 CC BY-NC 4.0 DEED Attribution-NonCommercial 4.0 International, 2026

DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. American Sociological Review, 48(2), 147–160. https://doi.org/10.2307/2095101

Doneda, D. (2021). Da privacidade à proteção de dados pessoais (2. ed.). Editora Renovar.

Eubanks, V. (2018). Automating inequality. St. Martin's Press.

European Data Protection Board. (2022). Guidelines 07/2020 on the concepts of controller and processor in the GDPR. EDPB. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en

European Union. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, L, 2024/1689.

Floridi, L., & Cowls, J. (2019). A unified framework of five principles for AI in society. Harvard Data Science Review, 1(1). https://doi.org/10.1162/99608f92.8cd550d1

International Organization for Standardization. (2023). ISO/IEC 42001:2023—Information technology—Artificial intelligence—Management system. Geneva, Switzerland: ISO.

Janssen, M., & Kuk, G. (2016). The challenges and limits of big data algorithms in technocratic governance. Government Information Quarterly, 33(3), 371–377. https://doi.org/10.1016/j.giq.2016.08.011

Lee, H. P., Sarkar, A., Tankelevitch, L., Drosos, I., Rintel, S., Banks, R., & Wilson, N. (2025). The impact of generative AI on critical thinking: Self-reported reductions in cognitive effort and confidence effects from a survey of knowledge workers. In Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems (pp. 1–22). https://doi.org/10.1145/3706598.3713778

Merton, R. K. (1936). The unanticipated consequences of purposive social action. American Sociological Review, 1(6), 894–904.

Meyer, J. W., & Rowan, B. (1977). Institutionalized organizations: Formal structure as myth and ceremony. American Journal of Sociology, 83(2), 340–363. https://doi.org/10.1086/226550

Motta, F. C. P., & Alcadipani, R. (1999). Jeitinho brasileiro, controle social e competição. Revista de Administração de Empresas, 39(1), 6–12. https://doi.org/10.1590/S0034-75901999000100002

Noble, S. U. (2018). Algorithms of oppression: How search engines reinforce racism. NYU Press. https://doi.org/10.2307/j.ctt1pwt9w5

OECD. (2023). OECD AI principles overview. OECD AI Policy Observatory. https://oecd.ai/en/ai-principles

Parker, C. (2002). The open corporation: Effective self-regulation and democracy. Cambridge University Press. https://doi.org/10.1017/CBO9780511550034

 CC BY-NC 4.0 DEED Attribution-NonCommercial 4.0 International, 2026

Parker, C., & Braithwaite, J. (2003). Regulation. In P. Cane & M. Tushnet (Eds.), The Oxford handbook of legal studies (pp. 119–145). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199248179.013.0007

Pelizza, A. (2020). Processing alterity, enacting Europe: Migrant registration and identification as co-construction of individuals and polities. Science, Technology, & Human Values, 45(2), 262–288. https://doi.org/10.1177/0162243919827927

Silva, X.; Ribeiro, Y. (2021) Digital governance and democratic oversight: The role of reflexive capacity in algorithmic auditing. Journal of Digital Constitutionalism;

UNESCO. (2021). Recommendation on the ethics of artificial intelligence. UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000381137

von Garrel, J., & Mayer, J. (2025). Künstliche Intelligenz im Studium — Eine quantitative Längsschnittstudie zur Nutzung KI-basierter Tools durch Studierende. Hochschule Darmstadt. https://opus4.kobv.de/opus4-h-da/frontdoor/index/index/docId/533

Whetten, D. A. (1989). What constitutes a theoretical contribution? Academy of Management Review, 14(4), 490–495.

Zuboff, S. (2019). The age of surveillance capitalism. PublicAffairs.

Author Contributions:

André Afonso Silva is the sole author and was responsible for conceptualization, methodology, analysis, and writing. The author has read and agreed to the published version of the manuscript.

About the Author

André Afonso Silva holds a degree in Systems and Computer Engineering from Rio de Janeiro State University (UERJ) and an M.Sc. from the Federal University of Rio de Janeiro (UFRJ). He is a public servant at UERJ, the founder of Essência A.I. Ltda., an AI governance consultancy, and Vice-Chair of the Council on Innovation, Digital Transformation and Deep Tech at the Federation of Foreign Trade Chambers (FCCE). His research addresses AI governance, institutional accountability, and data protection, with particular attention to the institutional conditions that precede regulatory compliance. In July 2026, his analytical series (Essência AI Insights) was listed in the Partnerships Hub of the United Nations Global Dialogue on AI Governance (Geneva).

 CC BY-NC 4.0 DEED Attribution-NonCommercial 4.0 International, 2026