RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Year VII, v.1 2026 | Submission: July 3, 2026 | Accepted: July 6, 2026 | Publication: July 9, 2026

Law and Technology in Dialogue: A Joint Analysis of the Impacts of Generative Artificial Intelligence on Privacy and Information Security in the Corporate Context

Direito e tecnologia em diálogo: uma análise conjunta dos impactos da inteligência artificial generativa na privacidade e segurança da informação no contexto corporativo

Derecho y tecnología en diálogo: un análisis conjunto de los impactos de la inteligencia artificial generativa en la privacidad y la seguridad de la información en el contexto corporativo

Manoel Pereira de Lima Junior
Juliana Beatriz Moraes Miura

Abstract:
The rapid expansion of Generative Artificial Intelligence (GAI) in the corporate environment poses new challenges to personal data protection, information security, and organizational governance. This article analyzes, from an interdisciplinary perspective, the legal, technological, and philosophical impacts arising from the use of GAI platforms by organizations, with emphasis on Brazil's General Data Protection Law (LGPD – Law No. 13,709/2018), the risks of confidential information leakage, and the challenges posed by the phenomenon known as Shadow AI. The investigation articulates principles of Digital Law with Information Security standards, internationally recognized technical norms (ISO/IEC 27001, ISO/IEC 42001, NIST AI RMF, OWASP LLM Top 10), and philosophical frameworks drawn from Michel Foucault, Zygmunt Bauman, Byung-Chul Han, and Shoshana Zuboff. As a result, it is demonstrated that the effective protection of corporate informational assets requires an integrated approach encompassing people, processes, technology, and organizational culture, transcending the dichotomy between technological innovation and legal compliance. A model of responsible GAI governance is proposed, grounded in Privacy by Design, Zero Trust, risk management, and digital ethics.

Keywords:
Generative Artificial Intelligence. LGPD. Information Security. Shadow AI. Data Governance. Privacy. Corporate Cybersecurity.

Resumo:
A rápida expansão da Inteligência Artificial Generativa (IAG) no ambiente corporativo impõe novos desafios à proteção de dados pessoais, à segurança da informação e à governança organizacional. O presente artigo analisa, sob perspectiva interdisciplinar, os impactos jurídicos, tecnológicos e filosóficos decorrentes do uso de plataformas de IAG pelas organizações, com ênfase na Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018), nos riscos de vazamento de informações confidenciais e nos desafios do fenômeno denominado Shadow AI. A investigação articula fundamentos do Direito Digital com princípios de Segurança da Informação, normas técnicas reconhecidas internacionalmente (ISO/IEC 27001, ISO/IEC 42001, NIST AI RMF, OWASP LLM Top 10) e referenciais filosóficos de Michel Foucault, Zygmunt Bauman, Byung-Chul Han e Shoshana Zuboff. Como resultado, demonstra-se que a proteção efetiva dos ativos informacionais corporativos exige uma abordagem integrada entre pessoas, processos, tecnologia e cultura organizacional, superando a dicotomia entre inovação tecnológica e conformidade jurídica. Propõe-se um modelo de governança responsável da IAG fundamentado em princípios de Privacy by Design, Zero Trust, gestão de riscos e ética digital.

Year VII, v.1 2026 | Submission: July 3, 2026 | Accepted: July 6, 2026 | Publication: July 9, 2026

Palavras-chave:
Inteligência Artificial Generativa. LGPD. Segurança da Informação. Shadow AI. Governança de Dados. Privacidade. Cibersegurança Corporativa.

Resumen:
La rápida expansión de la Inteligencia Artificial Generativa (IAG) en el entorno corporativo impone nuevos desafíos a la protección de datos personales, la seguridad de la información y la gobernanza organizacional. El presente artículo analiza, desde una perspectiva interdisciplinaria, los impactos jurídicos, tecnológicos y filosóficos derivados del uso de plataformas de IAG por las organizaciones, con énfasis en la Ley General de Protección de Datos de Brasil (LGPD – Ley n.º 13.709/2018), en los riesgos de filtración de información confidencial y en los desafíos del fenómeno denominado Shadow AI. La investigación articula fundamentos del Derecho Digital con principios de Seguridad de la Información, normas técnicas reconocidas internacionalmente (ISO/IEC 27001, ISO/IEC 42001, NIST AI RMF, OWASP LLM Top 10) y referentes filosóficos de Michel Foucault, Zygmunt Bauman, Byung-Chul Han y Shoshana Zuboff. Como resultado, se demuestra que la protección efectiva de los activos informacionales corporativos exige un enfoque integrado entre personas, procesos, tecnología y cultura organizacional, superando la dicotomía entre innovación tecnológica y conformidad jurídica. Se propone un modelo de gobernanza responsable de la IAG fundamentado en principios de Privacy by Design, Zero Trust, gestión de riesgos y ética digital.

Palabras clave:
Inteligencia Artificial Generativa. LGPD. Seguridad de la Información. Shadow AI. Gobernanza de Datos. Privacidad. Ciberseguridad Corporativa.

INTRODUCTION

Generative Artificial Intelligence (GAI) [1]has emerged as one of the most disruptive technological innovations of the 21st century. Large Language Models (LLMs) , such as OpenAI's GPT-4, Google's Gemini, and Anthropic 's Claude , have become accessible to the general public and have rapidly penetrated corporate environments, transforming work processes, organizational communication, legal analysis, software development, and strategic management (BOMMASANI et al., 2021).

This technological penetration, while bringing undeniable benefits in productivity and innovation, carries with it risk factors that transcend purely technical dimensions. In the legal sphere, the use of public IAG platforms by employees and organizations raises fundamental questions about the processing of personal data, the civil and administrative liability of data controllers, and compliance with the Brazilian regulatory framework for data protection—the

[1]The term "Generative Artificial Intelligence" (GAI) refers to AI systems capable of producing new content—text, images, audio, code—from patterns learned in large volumes of data. It is distinguished from discriminative AI, which classifies or predicts categories in existing data.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Year VII, v.1 2026 | Submission: July 3, 2026 | Accepted: July 6, 2026 | Publication: July 9, 2026

General Data Protection Law (LGPD), Law No. 13.709, of August 14, 2018 (BRAZIL, 2018). This regulatory framework was inspired by the European General Data Protection Regulation (GDPR) [2]and represents the main legal instrument for privacy protection in Brazil.

In the field of information security, the unmanaged adoption of AI tools by employees—a phenomenon known as Shadow AI—represents a threat to the confidentiality, integrity, and availability of organizations' information assets. Strategic data, trade secrets, customer information, and intellectual property can be inadvertently inserted into models trained and maintained by third parties, with potentially irreversible consequences (GARTNER, 2023).

Given this scenario, this article proposes the following research problem: how can organizations balance the benefits provided by Generative Artificial Intelligence with the need for legal data protection, information security, and preservation of their strategic assets?

The justification for this investigation lies in the urgency and relevance of the topic. Brazil, despite having data protection legislation comparable in scope to the European GDPR, still lacks specific regulations on the use of artificial intelligence, making an integrated analysis of existing regulatory frameworks and international best practices indispensable. The execution of such tasks falls primarily to the National Data Protection Authority (ANPD) [3], which has been gradually expanding its regulatory role in this area.

The overall objective of this research is to analyze the legal, technological, and philosophical impacts of Generative Artificial Intelligence on privacy and information security in the corporate context. The specific objectives are: (a) to examine the regulatory framework of the LGPD (Brazilian General Data Protection Law) and its application to the use of GI; (b) to identify the main information security risks associated with the corporate use of GI; (c) to analyze the Shadow AI phenomenon and its governance challenges; (d) to articulate philosophical foundations on power, data, and surveillance within the context of GI; and (e) to propose guidelines for responsible governance of GI in the corporate environment.

The methodology adopted is bibliographic, exploratory, and qualitative, based on a review of scientific literature, applicable legislation, technical standards, and institutional documents, as outlined in the specific methodological section.

---

[2]The GDPR (General Data Protection Regulation (EU) 2016/679 entered into force on 25 May 2018 and is considered the global benchmark for personal data protection, having directly influenced the drafting of the Brazilian LGPD.

[3]The ANPD (National Data Protection Authority) was created by Decree No. 10,474/2020 as a special-purpose autonomous agency linked to the Presidency of the Republic, endowed with technical and decision-making autonomy, its own assets, and specific revenues. It is responsible for ensuring the protection of personal data, developing guidelines for the National Data Protection Policy, and monitoring and applying sanctions.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Year VII, v.1 2026 | Submission: July 3, 2026 | Accepted: July 6, 2026 | Publication: July 9, 2026

Evolution of Generative Artificial Intelligence in the Corporate Environment

The trajectory of Artificial Intelligence spans decades of scientific advancements and paradigm shifts. From the first symbolic models and expert systems of the 1950s and 1960s, through artificial neural networks and supervised machine learning, we arrived at the deep learning paradigm , which revolutionized the computational capabilities of natural language processing, computer vision, and content generation (GOODFELLOW; BENGIO; COURVILLE, 2016). The transformative milestone for AI was the introduction of the Transformer architecture [4], proposed by Vaswani et al. (2017) in the seminal article " Attention ". Is All You Need ".

This architecture enabled the training of models on an unprecedented scale, culminating in the development of LLMs that characterize the current generation of AI tools. The fine-tuning process through Reinforcement Learning from Human Feedback (RLHF) [5]has made these models more aligned with user expectations. The public launch of ChatGPT in November 2022 represented a turning point: in less than five days, the platform reached one million users, and in two months, one hundred million — an unprecedented speed of adoption in the history of consumer technology (OPENAI, 2023).

In the corporate environment, IAG penetration occurred across multiple dimensions. Legal departments began using LLMs for contract review and case law research; technology teams adopted code generation tools; marketing departments explored automated content creation; and managers used the tools for report synthesis and decision support (MCKINSEY GLOBAL INSTITUTE, 2023).

According to a McKinsey Global Institute report (2023), AI has the potential to automate activities that account for 60% to 70% of employees' current working time in various cognitive functions. This transformative potential, however, coexists with risks that most organizations are not yet prepared to manage adequately.

---

[4]Transformer architecture model , introduced by Vaswani et al. (2017), utilizes attention mechanisms (attention). mechanisms that allow the model to weigh the relevance of different parts of the input text when generating each output token. This architecture overcomes the limitations of recurrent nesting networks (RNNs) and allows for massively scaled parallelization of training.

[5]The RLHF (Reinforcement Learning from Human Feedback (RLHF) is a fine-tuning technique for LLMs in which human raters rate the model's responses, and this rating is used to train a reward model that guides the LLM's reinforcement learning. RLHF has been fundamental in making models like ChatGPT more aligned with user expectations and preferences.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Year VII, v.1 2026 | Submission: July 3, 2026 | Accepted: July 6, 2026 | Publication: July 9, 2026

Gartner (2023) identified that, by 2025, more than 80% of companies will have implemented AI applications in their processes—but less than 30% will have established adequate policies and controls to mitigate the associated risks. This asymmetry between adoption and governance constitutes the core of the problem investigated in this article.

Data as a New Strategic Asset for Organizations

The rise of the digital economy has radically transformed the nature and value of data. Previously treated as a byproduct of organizational operations, data has become the primary strategic asset of 21st-century businesses. The expression popularly attributed to the British economist Clive Humby — "data is "The new oil " — summarizes, albeit in a simplified way, the centrality that structured and unstructured information has acquired in the creation of economic value (THE ECONOMIST, 2017).

In the corporate context, data takes on multiple strategic categories: customer data (purchase history, preferences, financial data), employee data (personal information, performance data, health records), intellectual property (source code, formulas, production processes), confidential financial information, and trade secrets. Each of these categories simultaneously represents a competitive asset and a legal liability—the unauthorized disclosure of which can generate significant financial, reputational, and legal damages.

Valuing data as a strategic asset has direct implications for corporate governance. Boards of Directors and Senior Management have come to recognize that data protection is not merely a technical or regulatory compliance issue, but a fundamental dimension of business strategy and risk management (WORLD ECONOMIC FORUM, 2020).

From this perspective, the arrival of IAG in the corporate environment creates a paradox: the same tools that allow for extracting value from data with unprecedented efficiency are, simultaneously, potential vectors for the leakage and unauthorized exposure of this information. When an employee enters sensitive corporate data into a public IAG platform to obtain analyses, suggestions, or summaries, they may be transferring this strategic asset to third-party servers—with potentially devastating legal and competitive consequences.

The classification and inventory of corporate data, therefore, become indispensable prerequisites for any AI governance strategy. Without knowing what data exists, where it resides, and its level of sensitivity, organizations cannot establish adequate controls over what can or cannot be processed by external artificial intelligence tools (ISO/IEC 27001, 2022).

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Year VII, v.1 2026 | Submission: July 3, 2026 | Accepted: July 6, 2026 | Publication: July 9, 2026

LEGAL ANALYSIS: LGPD, PRIVACY AND CORPORATE RESPONSIBILITY

The General Data Protection Law (LGPD), enacted on August 14, 2018, and in force since September 2020, represents the main Brazilian regulatory framework for the processing of personal data. Inspired by the European Union's General Data Protection Regulation (GDPR – Regulation 2016/679), the LGPD establishes principles, rights of data subjects, obligations of data processing agents, and administrative sanctions applicable by the regulatory body — the ANPD.

Article 6 of the LGPD (Brazilian General Data Protection Law) lists the principles that should guide the processing of personal data, with particular relevance to the context of IAG: purpose (processing for legitimate, specific, explicit purposes informed to the data subject); adequacy (compatibility with the informed purposes); necessity (limitation to the minimum necessary for the purpose); free access; data quality; transparency; security; prevention; non-discrimination; and accountability (BRAZIL, 2018, art. 6).

Regarding the legal bases for processing personal data, Article 7 of the LGPD (Brazilian General Data Protection Law) lists the circumstances that authorize processing, among which the consent of the data subject, the legitimate interest of the controller, and compliance with a legal obligation stand out. For sensitive personal data [6]—a category that includes data on health, sexual orientation, religious beliefs, genetic and biometric data—Article 11 of the LGPD imposes even stricter restrictions, generally requiring the specific and explicit consent of the data subject.

The insertion of personal data into public IAG platforms without an adequate legal basis, without specific contractual clauses with suppliers, and without a data protection impact assessment may constitute an infraction of the LGPD (Brazilian General Data Protection Law) subject to sanctions that include warnings, a simple fine of up to 2% of the company's revenue in Brazil (limited to R$ 50 million per infraction), daily fines, public disclosure of the infraction, blocking or deletion of the personal data involved (BRAZIL, 2018, art. 52).

The civil liability of organizations in the context of IAG (Intelligent Data Management) presents particularly complex dimensions. Article 42 of the LGPD (Brazilian General Data Protection Law) stipulates that the controller or operator who, due to the exercise of personal

[6]Sensitive personal data is defined by Article 5, II, of the LGPD (Brazilian General Data Protection Law) as data "concerning racial or ethnic origin, religious beliefs, political opinions, membership in a trade union or religious, philosophical or political organization, data concerning health or sex life, genetic or biometric data, when linked to a natural person".

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Year VII, v.1 2026 | Submission: July 3, 2026 | Accepted: July 6, 2026 | Publication: July 9, 2026

data processing activities, causes patrimonial, moral, individual or collective damage to the data subject, is obliged to repair it. The issue of the distribution of responsibility between the controller (the organization that defines the purposes of the processing) and the operator (the IAG platform provider) is a topic that demands special attention in service contracts.

From this perspective, the Shadow AI phenomenon can lead an organization to assume the role of controller of data processing that it is not even aware it is carrying out. This highlights the need for clear policies, control mechanisms, and internal awareness programs.

The international transfer of data represents another critical legal dimension. The main providers of public AGI platforms — OpenAI, Google, Microsoft, Anthropic — are US companies, whose servers largely reside outside of Brazilian territory. Article 33 of the LGPD (Brazilian General Data Protection Law) conditions the international transfer of personal data on the existence of an adequate level of protection in the destination country (to be recognized by the ANPD - National Data Protection Authority), the existence of specific contractual guarantees, or other exhaustive hypotheses (ANPD, 2023).

The ANPD (National Data Protection Authority) has made progress in publishing relevant guidelines for the context of AI. However, specific regulations on AI are still under development within the Brazilian legislative process—notably Bill No. 2,338/2023 [7], which is being processed in the Federal Senate and proposes a specific regulatory framework for artificial intelligence in Brazil.

Within the scope of administrative liability, the ANPD (National Data Protection Authority) can initiate administrative sanctioning proceedings against organizations that use AI platforms without complying with the requirements of the LGPD (Brazilian General Data Protection Law). Demonstrating the adoption of technical and organizational security measures—and the existence of a robust privacy governance program—are factors that can mitigate the liability of data processing agents (BRAZIL, 2018, art. 50).

TECHNOLOGICAL ANALYSIS: RISKS, VULNERABILITIES AND SECURITY CONTROLS

[7]Bill No. 2,338/2023, authored by Senator Rodrigo Pacheco, proposes a comprehensive regulatory framework for artificial intelligence in Brazil, based on a risk-based approach similar to the EU AI Act . The bill classifies AI systems into three risk categories—unacceptable, high, and limited—and establishes differentiated obligations for each category, including compliance assessments, transparency, and human oversight.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Year VII, v.1 2026 | Submission: July 3, 2026 | Accepted: July 6, 2026 | Publication: July 9, 2026

From an information security perspective, Generative Artificial Intelligence represents a multidimensional risk vector that challenges traditional corporate protection models. To properly understand these risks, it is necessary to analyze the technical functioning of LLMs (Learning Management Tools) and their inherent vulnerabilities, as well as the risks associated with the unmanaged corporate use of these tools.

LLMs are trained on vast textual datasets using deep learning techniques based on the Transformer architecture. Once trained, these models are tuned with additional data and techniques such as RLHF to align their behavior with user expectations. The inference process—the generation of real-time responses—occurs on the provider's servers, meaning that every prompt sent by the user is transmitted and processed on the third-party infrastructure (OUYANG et al., 2022).

In 2023, OWASP (Open Web Application Security Project) published the "OWASP Top 10 for Large Language Model Applications ," a document that catalogs the main security vulnerabilities of LLM- based systems . The most relevant to the corporate context include: Prompt Injection (manipulation of model behavior through malicious instructions inserted into prompts); leakage of sensitive data contained in the conversation context; training with poisoned data (data poisoning); generation of unreliable content—so-called "hallucinations" [8]—with the potential to cause harm; and excessive reliance on model outputs without adequate human validation (OWASP, 2023).

Regarding the risk of exposure of confidential information, studies conducted by security companies such as Cyberhaven and LayerX Security (2023) revealed that a significant portion of the data entered by employees on public IAG platforms contains sensitive corporate information. The Samsung episode [9]in March 2023 became emblematic: company engineers inserted proprietary source code into ChatGPT for debugging, resulting in the potential exposure of trade secrets (BUSINESSINSIDER, 2023).

The ISO/IEC 27001:2022 standard, which specifies the requirements for establishing, implementing, maintaining, and continuously improving an Information Security Management

[8]The phenomenon of "hallucinations" in LLMs refers to the generation of factually incorrect information, non-existent bibliographic references, or unverifiable statements presented with apparent confidence by the model. This phenomenon is a consequence of the statistical nature of LLMs , which generate tokens based on probabilities, without access to an internal truth model or factual verification.

[9]In March 2023, Samsung Semiconductor employees inserted proprietary source code into ChatGPT on at least three separate occasions: for debugging database code, for verifying code related to semiconductor equipment, and for converting meeting notes into presentations. Samsung subsequently banned the use of external generative AI tools on its corporate devices.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Year VII, v.1 2026 | Submission: July 3, 2026 | Accepted: July 6, 2026 | Publication: July 9, 2026

System (ISMS), provides the structural framework for managing these risks. Annex A of the standard lists security controls organized into four categories—organizational, human, physical, and technological—which, applied to the IAG context, imply the need for acceptable use policies, employee training, supplier evaluation, and technical data loss controls. Prevention (DLP) and management of specific vulnerabilities in AI-based applications (ISO/IEC 27001, 2022). The ISO/IEC 42001:2023 standard [10]complements this framework with specific requirements for artificial intelligence management systems.

Zero Trust architecture [11], formalized by NIST in special publication SP 800-207 (2020), is based on the principle that no user, device, or service should be considered trusted by default. Applied to the context of IAG, this implies that access to IAG tools should be granted based on explicit authorization policies, continuous identity verification, and behavior monitoring, with the minimum privileges necessary for the function performed.

and Data Loss solutions[12] Prevention (DLP) completes the technical arsenal available for mitigating the risks of enterprise AI. Finally, the deployment of private and secure environments for enterprise AI—such as on-premises or private cloud instances of language models—allows organizations to enjoy the benefits of AI without exposing sensitive data to third parties (MICROSOFT, 2023).

Shadow AI **and the New Governance Challenges**

The concept of Shadow IT, referring to the use of information technology systems without the explicit approval of the corporate IT department, is a phenomenon widely studied in the IT management literature since the 1980s (SILIC; BACK, 2014). With the spread of public AI platforms, a contemporary and particularly dangerous manifestation of this

[10]ISO/IEC 42001:2023 is the first international management system standard specifically dedicated to artificial intelligence. It establishes requirements and provides guidance for organizations that develop, supply, or use AI systems responsibly, addressing aspects such as governance, risk management, impact on human rights, transparency, and continuous improvement.

[11]A Zero Trust Architecture (ZTA), as defined by NIST SP 800-207, is based on three fundamental principles: (1) all data sources and computing services are considered resources; (2) all (3) communication is protected regardless of location on the network; (4) access to individual resources is granted per session, with continuous verification of identity and context.

[12]A Cloud Access Security Broker (CASB) is a security solution positioned between enterprise users and cloud service providers, applying security policies to data traffic in real time. Key functions of a CASB include visibility into cloud service usage, access control, threat protection, and regulatory compliance.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Year VII, v.1 2026 | Submission: July 3, 2026 | Accepted: July 6, 2026 | Publication: July 9, 2026

phenomenon has emerged: Shadow AI, characterized by the use of AI tools by employees without the knowledge, approval, or control of the organization.

Shadow AI presents a unique governance challenge compared to traditional Shadow IT. Firstly, the barrier to entry is virtually nonexistent: high-powered AI tools are available for free or at marginal cost, accessible through any internet-connected device, without the need for software installation or network configuration. Secondly, the potential consequences are immediate and possibly irreversible: data entered into external AI platforms can be used to retrain models, making their subsequent recovery virtually impossible.

Research conducted by Cyberhaven (2023) analyzed the behavior of over 1.6 million employees and found that 11% of the data entered into IAG tools was sensitive corporate data , notably source code, financial data, business strategies, and internal communications. A study by LayerX Security (2023) revealed that only 8% of the organizations surveyed had effective controls to monitor and control the use of IAG by their employees.

Shadow AI risk vectors can be categorized into three dimensions: (a) confidentiality risk, due to the exposure of sensitive information and intellectual property to external providers without an adequate contractual basis; (b) legal risk, due to the potential for violation of the LGPD (Brazilian General Data Protection Law) and contractual confidentiality clauses with clients and partners; and (c) integrity and reliability risk, due to decision-making based on outputs from unvalidated, potentially inaccurate, or biased models.

From a governance perspective, addressing Shadow AI requires a simultaneously preventive, detective, and corrective approach. Preventive measures include establishing clear policies for the acceptable use of AI tools, communicated and trained to all employees; making approved corporate alternatives available; and creating agile processes for evaluating and approving new tools. Detective measures include monitoring network traffic to identify access to unapproved AI platforms. Corrective measures involve incident response, damage assessment, and adapting processes and controls.

It is crucial that the Shadow AI governance approach is not perceived by employees as merely restrictive or punitive. Literature on change management and organizational behavior demonstrates that outright prohibitions, without adequate alternatives, tend to increase employee resistance and encourage more sophisticated clandestine behaviors (SILIC; BACK, 2014). Effective Shadow AI governance, therefore, must balance control and enablement.

DIALOGUE BETWEEN LAW AND TECHNOLOGY

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Year VII, v.1 2026 | Submission: July 3, 2026 | Accepted: July 6, 2026 | Publication: July 9, 2026

The relationship between Law and Technology has historically been marked by temporal asymmetries: legal regulation tends to arrive after the consolidation of technological phenomena, resulting in normative gaps that economic agents exploit to the detriment of individuals and the community. In the context of IAG (Innovation and Technology Management), this regulatory lag is particularly pronounced.

The dialogue between Law and Technology in the field of AI requires overcoming significant epistemological barriers. Lawyers, in their traditional training, are not equipped to understand the technical mechanisms of LLMs ; engineers and data scientists, in turn, are often unaware of the legal requirements and implications of their design decisions. Building bridges between these domains of knowledge is a sine qua non. essential for the development of effective IAG governance.

In the Brazilian regulatory framework, the LGPD (Brazilian General Data Protection Law) provides the main legal basis for addressing the risks of automated data handling (AGM) to the informational assets of organizations. Article 20 of the LGPD, which guarantees the data subject the right to request a review of decisions made solely on the basis of automated processing of personal data, represents a particularly relevant standard for the context of AGM applied to corporate decision-making processes.

Internationally, the European Union's Artificial Intelligence Regulation (EU AI Act) [13], approved in 2024, represents the first comprehensive regulatory framework specifically aimed at AI systems. Although not binding on Brazil, the AI Act influences global AI regulation and serves as an important reference for the Brazilian legislative process (EUROPEAN PARLIAMENT, 2024).

The interdisciplinary perspective between Law and Technology reveals that the legal protection of data in the context of IAG cannot be reduced to formal compliance with the LGPD (Brazilian General Data Protection Law). In this sense, the principle of Privacy The concept of data protection by design [14], articulated by Ann Cavoukian (2009) and incorporated into the regulatory framework of the European GDPR and, implicitly, into article 46 of the LGPD,

[13]The EU AI Act (Regulation (EU) 2024/1689) classifies the following as unacceptable risk AI systems, prohibited in the European Union: social scoring systems by public authorities; exploitation of vulnerabilities in specific groups; real-time remote biometric identification in public spaces (with limited exceptions); subliminal manipulation; and biometric categorization systems based on sensitive characteristics.

[14]Privacy Principle Privacy by Design was developed by Ann Cavoukian , former Information and Privacy Commissioner of Ontario (Canada), and establishes seven fundamental principles: proactive rather than reactive; privacy as the default setting; privacy built into the design; full functionality (positive sum, not zero sum); end-to-end security; visibility and transparency; and respect for user privacy.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Year VII, v.1 2026 | Submission: July 3, 2026 | Accepted: July 6, 2026 | Publication: July 9, 2026

establishes that data protection must be incorporated into the design of systems and processes from their conception, and not treated as an external element of compliance.

Philosophical Reflections on Power, Data, and Artificial Intelligence

An analysis of the impacts of information abuse on privacy and information security in the corporate context cannot disregard a philosophical foundation that situates the phenomenon within its broader dimension—the power relations that permeate the production, control, and exploitation of knowledge and information in contemporary society.

Michel Foucault, in "Discipline and Punish" (1975), describes the Benthamian panopticon [15]as a metaphor for modern disciplinary society—an architecture of surveillance in which the observer's gaze, even if potentially absent, induces in the observed a permanent awareness of their visibility, producing an effect of self-control and docility. AI, with its capacity to process and analyze massive amounts of behavioral data, represents a radically new and more sophisticated form of panopticism—no longer located in an observation tower, but ubiquitously distributed throughout the digital infrastructures of organizations and society (FOUCAULT, 1975).

The Foucauldian concept of biopower [16]—power over life, acting on individual bodies and populations—finds its contemporary expression in algorithmic systems that classify, segment, and condition the behavior of consumers, workers, and citizens. By inferring behavioral patterns, psychological tendencies, and identity categories from seemingly neutral data, algorithmic biopower exerts a form of algorithmic biopower that operates with unprecedented efficiency and scale in human history.

Zygmunt Bauman , with his concept of liquid modernity, offers a fundamental framework for understanding the fragility of social and institutional structures in the face of the speed of technological transformations. In "Liquid Modernity" (2001), Bauman describes a social condition marked by instability, the ephemerality of bonds, and the dissolution of the

[15]The panopticon, designed by Jeremy Bentham in the 18th century, is a circular prison architecture with a central watchtower, in which the guard can observe all the prisoners without being seen. Foucault uses this metaphor to describe the functioning of modern disciplinary institutions—prisons, schools, hospitals, factories—in which the awareness of the possibility of being observed is sufficient to produce the effect of self-control.

[16]The concept of "biopower" was developed by Foucault in the first volume of "The History of Sexuality" (1976) and in courses at the Collège de France. Biopower manifests itself in two forms: the anatomo-politics of the human body (discipline of individual bodies) and the biopolitics of the population (regulation of the biological processes of populations). Analytical AI represents a new technology of biopower that operates on an unprecedented scale and granularity.

solid structures that once organized social and political life. In the context of IAG, liquidity manifests itself in the speed with which new models and platforms emerge and spread, rendering regulatory frameworks and governance practices obsolete even before their consolidation (BAUMAN, 2001).

Byung-Chul Han analyzes the paradoxes of hyperconnectivity and the voluntary exposure of data. According to Han, contemporary society is characterized by a compulsion towards transparency and visibility—individuals and organizations voluntarily expose personal and strategic information on digital platforms, driven by the logic of performativity and optimization. This drive towards transparency, in Han's perspective, does not represent the emancipation promised by technological rhetoric, but rather a new form of control—more effective because it is internalized and seemingly voluntary (HAN, 2017).

In "The Age of Surveillance Capitalism" (2019), [17]Shoshana Zuboff provides the analysis most directly relevant to the context of corporate surveillance capitalism. Zuboff describes surveillance capitalism as a new economic logic that transforms human experience into raw material for behavioral products and services. For Zuboff, large technology platforms—and surveillance capitalism providers paradigmatically fit into this category—extract behavioral data from users without adequate compensation, process it to predict and influence future behaviors, and monetize it in the "behavioral futures market" (ZUBOFF, 2021).

The articulation of these philosophical frameworks reveals that the challenges of artificial intelligence (AI) for privacy and information security are not merely technical or legal—they are fundamentally political and ethical. The question of who controls the data, for what purposes, and with what consequences for individual and collective autonomy is, ultimately, a question of power—and its answer requires not only regulation and technology, but a profound ethical reflection on the values that should guide the development and use of artificial intelligence.

Proposals for Safe and Responsible AI Governance

Based on the interdisciplinary analysis developed in the preceding sections, this section presents a set of proposals for building a secure and responsible AI governance model within

[17]Zuboff coined the term "surveillance capitalism" to describe a new economic logic emerging from Google's practices, which discovered that users' behavioral data—originally a byproduct of searches—could be used to predict and influence future behaviors, creating a highly lucrative market for behavioral advertising. This logic was later adopted by Facebook and other digital platforms.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Year VII, v.1 2026 | Submission: July 3, 2026 | Accepted: July 6, 2026 | Publication: July 9, 2026

the corporate environment. In terms of corporate governance, it proposes the creation of an AI Governance structure that integrates representatives from the legal, information security, technology, human resources, compliance, and senior management areas. The ISO/IEC 42001:2023 standard [18]provides the structural framework for this governance.

In terms of legal and compliance, it is proposed that a Data Protection Impact Assessment (DPIA) be carried out [19], as provided for in Article 38 of the LGPD (Brazilian General Data Protection Law), for each case of significant use of AI involving personal data. Additionally, contracts with AI platform providers should include specific clauses on data processing, confidentiality, prohibition of data use for model retraining, incident notification, and civil liability.

In terms of technology, the proposal involves implementing a security architecture based on Zero Trust principles, with specific controls for the use of IAG: DLP policies configured to identify and block the transmission of sensitive data to non-approved IAG platforms; CASB solutions for monitoring and controlling the use of cloud-based IAG services; rigorous identity and access management (IAM) for approved corporate IAG tools; and preferential implementation of private IAG environments for use cases involving sensitive data.

In terms of organizational culture and people management, it is proposed to develop an ongoing awareness and training program on the responsible use of AI tools, addressing security risks, legal obligations arising from the LGPD (Brazilian General Data Protection Law), corporate acceptable use policies, and approved tools available to meet employee needs.

From an ethical standpoint, it is proposed to adopt a set of principles for the responsible use of AI in the corporate environment, aligned with the European Union's ethical guidelines for trustworthy AI (EUROPEAN COMMISSION, 2019) and the OECD principles on AI (OECD, 2019): human oversight and control; transparency and explainability; algorithmic fairness and non-discrimination; data privacy and security; responsibility and accountability; and social benefit and environmental sustainability.

---

[19]The Data Protection Impact Assessment (DPIA), also known as Data Protection Data Impact Assessment (DPIA), as required by Article 38 of the LGPD (Brazilian General Data Protection Law), is mandated when data processing may pose risks to civil liberties and fundamental rights. The ANPD (Brazilian National Data Protection Authority) may establish the circumstances under which a DPIA will be mandatory.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Year VII, v.1 2026 | Submission: July 3, 2026 | Accepted: July 6, 2026 | Publication: July 9, 2026

Finally, the proposal encourages the active engagement of organizations in regulatory development processes, contributing their practical experience to the development of regulatory frameworks that are both protective of fundamental rights and promote responsible innovation.

METHODOLOGY

This article adopts a bibliographic, exploratory, and qualitative research methodology, based on a review of scientific literature, applicable legislation, technical standards, and institutional documents.

The bibliographic research encompassed reference works in the fields of Law, Digital Law, Information Security, Philosophy of Technology, and Corporate Governance, with an emphasis on publications from the last ten years, without prejudice to classic works of philosophical reference. The databases consulted included the CAPES Periodicals Portal, Google Scholar, the Brazilian Digital Library of Theses and Dissertations (BDTD), and institutional repositories of national and international universities.

The review of technical and regulatory literature covered the main relevant international standards and frameworks: ISO/IEC 27001:2022, ISO/IEC 27002:2022, ISO/IEC 42001:2023, NIST Cybersecurity Framework (2018), NIST AI Risk Management Framework (2023), and OWASP Top 10 for LLM Applications (2023). Applicable Brazilian and foreign legislation was examined in full, with special attention to the LGPD (Brazilian General Data Protection Law) and the EU AI Act .

The exploratory nature of the research stemmed from the relative novelty of the phenomenon investigated and the scarcity of specific empirical studies on the corporate use of AI in the Brazilian context. The qualitative approach allowed for the interpretative and critical analysis of the collected data, with an emphasis on building interdisciplinary connections between the fields of Law, Technology, and Philosophy.

The methodological procedure adopted comprised: (a) survey and selection of relevant literature; (b) critical analysis of the selected texts; (c) synthesis and interdisciplinary articulation of the contents; (d) formulation of proposals based on the analysis performed. The bibliographic references were organized and formatted according to ABNT NBR 6023:2018 standards.

FINAL CONSIDERATIONS

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Year VII, v.1 2026 | Submission: July 3, 2026 | Accepted: July 6, 2026 | Publication: July 9, 2026

The analysis developed throughout this article shows that Generative Artificial Intelligence simultaneously represents one of the most powerful innovation tools available to contemporary organizations and a vector of legal, technological, and organizational risk of unprecedented magnitude. The tension between these two poles, innovation and risk, cannot be resolved by simple technological adoption or isolated regulation, but requires a truly integrated approach.

The proposed research problem does not allow for a simple or universal answer. Each organization has a unique risk profile, its own organizational culture, and a specific regulatory context. Nevertheless, the principles and practices identified in this research offer a consistent framework for building contextualized and effective responses.

Legal analysis has shown that the LGPD (Brazilian General Data Protection Law), although not specifically drafted for IAG's context, provides a sufficiently robust set of principles and regulatory instruments to govern the corporate use of these tools—provided that it is interpreted and applied creatively and contextually. The responsibility of organizations is not limited to formal compliance with legal requirements, but also includes adopting a proactive stance in protecting the rights of data subjects.

Technological analysis revealed that the risks of IAG to information security are real and potentially devastating, but are manageable through appropriate technical and organizational controls. Zero Trust architecture, DLP and CASB solutions, rigorous identity and access management, and the deployment of private IAG environments represent the state of the art in available technical controls.

Philosophical analysis has revealed that the challenges of human-centered intelligence (HCI) transcend technical and legal dimensions, situated in the realm of power relations, surveillance, the commodification of human experience, and the erosion of individual and collective autonomy. The frameworks of Foucault, Bauman , Han, and Zuboff offer indispensable critical lenses for understanding the deeper implications of HCI.

The fundamental conclusion of this research is that effective protection against IAG risks does not depend solely on technology or legislation in isolation, but on the integration of people, processes, governance, security, and organizational culture. Organizations that build this integration consistently and sustainably will not only comply with legal requirements and security best practices—they will also be better positioned to extract the real value that IAG has to offer, in a responsible, ethical, and sustainable way.

The path ahead demands collective effort: from organizations, in developing robust governance programs for generative artificial intelligence (GAI); from the Legislative Branch,

in building specific and appropriate regulatory frameworks; from the National Data Protection Authority (ANPD), in regulating and guiding data processing agents; from academia, in producing rigorous interdisciplinary knowledge; and from civil society, in monitoring and defending fundamental rights threatened by the irresponsible use of these technologies. Generative artificial intelligence is, ultimately, a mirror of human intelligence—and the choices we make about how to develop and use it reflect, for better or for worse, the values that we as a society decide to prioritize.

REFERENCES

NATIONAL DATA PROTECTION AUTHORITY (ANPD). Guidance Guide on International Transfer of Personal Data. Brasília: ANPD, 2023. Available at: https://www.gov.br/anpd. Accessed on: June 8, 2026.

BAUMAN, Zygmunt. Liquid Modernity. Translated by Plínio Dentzien . Rio de Janeiro: Zahar, 2001.

BOMMASANI, Rishi et al. On the Opportunities and Risks of Foundation Models. Stanford CRFM, 2021. Available at: https://arxiv.org/abs/2108.07258. Accessed on: 8 June. 2026.

BRAZIL. Law No. 13.709, of August 14, 2018. General Law on the Protection of Personal Data (LGPD). Official Gazette Official Gazette of the Union : Section 1, Brasília, DF, August 15, 2018.

BUSINESSINSIDER. Samsung workers accidentally leaked trade secrets while using ChatGPT. Business Insider, 2023. Available at: https://www.businessinsider.com/samsung-workers-leaked-trade-secrets-chatgpt-2023-4. Access 8 June 2026.

CAVOUKIAN, Ann. Privacy by Design: The 7 Foundational Principles. Ontario: Information and Privacy Commissioner of Ontario, 2009.

CYBERHAVEN. Cyberhaven 1 Million User Study: How Employees Use ChatGPT and Other AI Tools at Work. San Francisco: Cyberhaven , 2023.

EUROPEAN COMMISSION. Ethics Guidelines for Trustworthy AI. Brussels : European Commission High-Level Expert Group on Artificial Intelligence, 2019.

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

FOUCAULT, Michel. Discipline and Punish: The Birth of the Prison. Translated by Raquel Ramalhete. Petrópolis : Vozes , 1987. (Original published) in 1975).

GARTNER. Top Strategic Technology Trends for 2024. Stamford: Gartner Research, 2023.

GOODFELLOW, Ian; BENGIO, Yoshua; COURVILLE, Aaron. Deep Learning. Cambridge: MIT Press, 2016.

HAN, Byung -Chul. The Transparency Society. Translated by Enio Paulo Giachini . Petrópolis: Vozes, 2017. (Original published in 2012).

HAN, Byung -Chul. In the Swarm: Perspectives on the Digital. Translated by Lucas Machado. Petrópolis: Vozes, 2018. (Original published) in 2013).

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection – Information security management systems – Requirements. Geneva : ISO, 2022.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 27002:2022 – Information security, cybersecurity and privacy protection – Information security controls. Geneva : ISO, 2022.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 42001:2023 – Artificial intelligence – Management system. Geneva : ISO, 2023.

LAYERX SECURITY. Annual Browser Security Report 2023. Tel Aviv: LayerX Security, 2023.

MCKINSEY GLOBAL INSTITUTE. The Economic Potential of Generative AI: The Next Productivity Frontier. New York: McKinsey & Company, 2023.

MICROSOFT. Azure OpenAI Service: Data, Privacy, and Security for Azure OpenAI Service. Redmond: Microsoft, 2023. Available at: https://learn.microsoft.com/azure/ai-services/openai/. Accessed [date] . 8 June 2026.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST AI 100-1. Gaithersburg: NIST, 2023.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. Gaithersburg: NIST, 2018.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). Zero Trust Architecture. NIST Special Publication 800-207. Gaithersburg: NIST, 2020.

OECD. Recommendation of the Council on Artificial Intelligence. OECD/LEGAL/0449. Paris: OECD, 2019.

OPENAI. GPT-4 Technical Report. San Francisco: OpenAI, 2023. Available at: https://arxiv.org/abs/2303.08774. Accessed On June 8, 2026.

OUYANG, Long et al. Training language models to follow instructions with human feedback. In: ADVANCES IN NEURAL INFORMATION PROCESSING SYSTEMS, 35., 2022. Proceedings [...]. NeurIPS , 2022.

OWASP FOUNDATION. OWASP Top 10 for Large Language Model Applications. Version 1.1. Wilmington: OWASP, 2023. Available at: https://owasp.org/www-project-top-10-for-large-language-model-applications/. Accessed on: June 8, 2026.

SILIC, Mario; BACK, Andrea. Shadow IT: A view from behind the curtain. Computers & Security, vol. 45, p. 274-283, 2014.

THE ECONOMIST. The world's most valuable resource is no longer oil, but data. The Economist, London, 6 May 2017.

VASWANI, Ashish et al. Attention Is All You Need. In: ADVANCES IN NEURAL INFORMATION PROCESSING SYSTEMS, 30., 2017. Proceedings [...]. NeurIPS , 2017.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Year VII, v.1 2026 | Submission: July 3, 2026 | Accepted: July 6, 2026 | Publication: July 9, 2026

WORLD ECONOMIC FORUM. Data Free Flow with Trust: Overcoming Barriers to Cross-Border Data Flows. Cologny /Geneva: World Economic Forum , 2020.

ZUBOFF, Shoshana . The Age of Surveillance Capitalism: The Struggle for a Human Future on the New Frontier of Power. Translated by George Schlesinger. Rio de Janeiro: Intrínseca, 2021. (Original published in 2019).