Scientific Research Publishing

Beijing Law Review, 2026, 17(1), 202-219
https://www.scirp.org/journal/blr
ISSN Online: 2159-4635
ISSN Print: 2159-4627

Artificial Intelligence and Violation of the LGPD: Corporate Liability for the Misuse of Data

Yasmin Santana Santos Gomes*

Department of Law, Pontifícia Universidade Católica do Rio de Janeiro, Salvador, Brazil
Email: *yasminssgomes@hotmail.com

How to cite this paper: Gomes, Y. S. S. (2026). Artificial Intelligence and Violation of the LGPD: Corporate Liability for the Misuse of Data. *Beijing Law Review, 17,* 202-219.
https://doi.org/10.4236/blr.2026.171012

Received: September 25, 2025
Accepted: March 9, 2026
Published: March 12, 2026

Abstract

The rise of Artificial Intelligence (AI) in the collection and processing of personal data poses significant legal challenges, particularly regarding compliance with the General Data Protection Law (LGPD). Decision-making automation, enabled by machine learning and deep learning, increases the need for traceability and transparency in the processing of personal information. However, algorithmic opacity and the biases embedded in predictive models hinder corporate accountability for potential privacy and data protection violations. Brazilian regulation still struggles to harmonize technological innovation with existing legal frameworks, as evidenced by recent issues related to automated decisions and leaks of sensitive data. The role of the National Data Protection Authority (ANPD) has been crucial in setting regulatory guidelines and best practices for AI governance, demanding greater corporate accountability in complying with the LGPD. Given the complexity of this issue, this study analyzes the civil liability of organizations for the misuse of AI in the processing of personal data, considering legal implications, regulatory challenges, and impacts on data subjects' rights. The research explores the need for specific regulation of high-risk AI, the strengthening of compliance measures, and the adoption of algorithmic audits as mechanisms to mitigate risks. It concludes that the balance between innovation and data protection requires policies of transparency, algorithmic explainability, and more robust regulatory oversight to ensure compliance with the principles of the LGPD.

Keywords

Artificial Intelligence, LGPD, Data Privacy, Compliance, Civil Liability, Algorithmic Governance

1. Introduction

The rise of Artificial Intelligence (AI) in the digital context represents a disruptive advance in the way personal data is collected, processed, and used. However, its wide applicability generates legal and regulatory challenges, especially concerning privacy protection and compliance with the normative principles established in the Brazilian General Data Protection Law—LGPD (Law No. 13.709/2018) (Wang et al., 2021). The regulation of data processing in Brazil, strongly inspired by the European Union's General Data Protection Regulation—GDPR, imposes strict obligations on data controllers, requiring a balance between technological innovation and respect for the fundamental rights of data subjects (Brazil, 2018).

The development of AI systems, particularly those operating through machine learning and deep learning, enhances the capacity for automated decision-making, reducing human interference in the processing of personal data. However, such decision-making autonomy, as pointed out by Fama (2024), creates a scenario where traceability and explainability of algorithmic decisions become a challenge, making it difficult to assess liability in cases of improper handling of information. Furthermore, the application of AI in the corporate sector has raised controversies regarding its compliance with the principles of purpose, transparency, and security established by the LGPD, which set limits on the manipulation of personal data without the informed consent of data subjects (Freire de Sá & Macena de Lima, 2021).

The increase in litigation related to the use of AI in data processing is an indicator that national jurisprudence has faced challenges in harmonizing technological innovations with the existing normative framework. The judgment of the Appeal in Case No. 0018165-45.2022.8.16.0021, by the 2nd Special Appeals Panel of the Paraná State Court of Justice (TJPR).

As reported by Veja magazine on October 22, 2025 (Veja, 2025), the largest data breach in the history of the Pix system occurred, exposing information linked to more than 11 million keys registered with the Central Bank. The episode highlights the vulnerability of digital infrastructures and the insufficiency of protection mechanisms in the face of the rapid advancement of technologies based on artificial intelligence. The incident, considered one of the largest in the country, exposed data such as names, CPF numbers, and banking information managed by the National Council of Justice (CNJ).

The unlawful disclosure of sensitive data reinforces the urgency of public policies and corporate measures that ensure compliance with the principles of security, transparency, and accountability established by the General Data Protection Law (Law No. 13,709/2018). This case, widely covered by the media, serves as a warning about the risks arising from the automated processing of personal information without adequate technical and legal safeguards, which amplifies the potential for moral and financial harm to data subjects.

Exemplifies this issue, recognizing that the absence of sufficient documentation to prove the leak of sensitive data prevented the attribution of liability to the com-

pany, even though the plaintiff alleged violations of fundamental rights (Brazil, 2023a). This decision reflects the need for more detailed regulation regarding the burden of proof in disputes involving AI and data protection, avoiding that normative gaps result in the impossibility of effectively protecting data subjects.

In the regulatory sphere, the National Data Protection Authority (ANPD) plays a crucial role in defining guidelines to mitigate risks arising from the misuse of AI in data management. According to Silva (2023a), ANPD's role is essential in setting technical parameters for security and accountability, enabling companies to implement compliance practices aligned with LGPD requirements. Infralegal regulation, through ANPD's votes and resolutions, can establish a minimum standard of diligence, which is fundamental for assigning objective or subjective liability to companies in cases of violations of data protection.

In this context, the present study aims to analyze the civil liability of companies for the misuse of personal data by AI systems, considering regulatory challenges and legal risks stemming from the interpretation and application of the LGPD in the context of automated decision-making. The research adopts a theoretical approach, with a doctrinal review and analysis of national jurisprudence, as well as a normative investigation of the legal provisions applicable to the subject.

The structure of this study is divided into specific chapters: Chapter 2 examines the relevant facts and implications of AI use in personal data processing, addressing concrete cases and social impacts. Chapter 3 deals with the legal issues and fundamental principles of the LGPD applicable to AI, exploring corporate obligations and the sanctions for noncompliance. Chapter 4 develops a detailed legal analysis based on the doctrine of Doneda, Bioni, and Peck Pinheiro, as well as the interpretation of superior courts regarding corporate liability in the use of AI. Chapter 5 discusses the practical application of legislation, with proposals for corporate best practices, compliance measures, and audits aimed at risk mitigation. Finally, Chapter 6 presents the final considerations, with recommendations for regulatory improvement and reflections on the need for a more robust legal framework for AI and the protection of personal data.

2. Description of Relevant Facts

According to Sichman (2021), there is no single academic definition of Artificial Intelligence (AI). However, he characterizes it as a branch of computer science and engineering aimed at developing computational systems capable of solving problems that are currently better resolved by human beings or that lack a viable algorithmic solution through conventional computing. AI therefore encompasses a variety of models, techniques, and technologies, including search, reasoning, knowledge representation, decision-making mechanisms, perception, planning, natural language processing, uncertainty management, and machine learning.

> Artificial Intelligence (AI), which emerged in the 1950s, has its origin practically intertwined with the origin of the computer itself. More precisely, in the summer of 1956, the Dartmouth College Conference took place, considered

> the founding milestone of AI. The researchers recognized as the fathers of the field, such as John McCarthy, Marvin Minsky, Alan Newell, and Herbert Simon, among others, participated in this event and developed scientific trajectories that established milestones in this fascinating domain of computing. As its very name suggests, the field has always been surrounded by enormous expectations, which in many cases were not fully achieved. As a result, the mood regarding the field has oscillated like a sine curve, with periods of great enthusiasm and funding (such as now) followed by times of disappointment and scarce resources. These downturns are known as AI Winters, such as those between 1975/1980 and 1987/1993. Currently, we are once again experiencing a period of euphoria regarding the possible benefits that AI can provide. Such optimism is justified by the conjunction of three fundamental factors: (i) the cost of processing and memory has never been so low; (ii) the emergence of new paradigms, such as deep neural networks, enabled by the first factor and producing undeniable scientific advances; and (iii) the vast amount of data available on the internet due to the widespread use of networks and social media. This enthusiasm, however, has also been accompanied by a series of fears, some of which are well-founded (Sichman, 2021: p. 37).

According to Costa and Bruno (2025), Artificial Intelligence (AI) has high disruptive potential, providing significant advances in process automation, predictive analytics, and the optimization of complex systems. Its use in machine learning and deep neural networks enables large-scale data modeling, increasing the accuracy of medical diagnoses, the efficiency of business decision-making, and the security of critical infrastructures. However, the authors emphasize that AI implementation requires strict measures of algorithmic governance, particularly with regard to mitigating biases in predictive models and preserving user privacy. Furthermore, the proliferation of technologies such as deepfakes and autonomous systems reinforces the need for regulation to prevent risks to information integrity and human decision-making control.

According to Abrantes (2023), algorithmic culture imposes dilemmas on personal data protection, since AI-based systems can generate detailed profiles of individuals, often without explicit consent. The General Data Protection Law (LGPD) and other regulations, such as the guidelines of the National Data Protection Authority (ANPD, 2024), aim to mitigate risks associated with automation in decision-making, but regulatory gaps still exist regarding algorithm transparency and liability for damages caused by failures or biases.

As Costa and Bruno (2025) emphasize, the use of AI must be accompanied by governance and algorithmic audit mechanisms to ensure that predictive models are used ethically and safely. Furthermore, Araújo (2022) highlights that the indiscriminate application of AI in the workplace can exacerbate risks of discrimination, digital harassment, and privacy invasion, making it essential to establish clear guidelines to limit the abusive use of these technologies.

Thus, the growing popularization of Artificial Intelligence (AI) in personal data processing has boosted the digitalization of services and the automation of decision-making processes across various economic sectors. However, this technological innovation also increases risks to privacy and data protection, since AI algorithms are capable of extracting, cross-referencing, and inferring sensitive information about individuals without direct human control over their operational logic (Lima & Sá, 2020). As highlighted by Fama (2024), AI systems operating with machine learning and deep learning present a high degree of autonomy, capable of generating behavioral and predictive profiles often without transparency regarding their decision-making criteria, which makes traceability and legal oversight over data processing more difficult.

The materialization of risks inherent in AI use has been evident in several episodes of personal data leaks, compromising not only the privacy of data subjects but also their financial and reputational integrity. A landmark case occurred in 2023, when a security flaw in an AI-based recruitment system resulted in the undue exposure of sensitive information from thousands of job applicants, including salary histories and performance evaluations (Ludgero, 2024). Similar episodes were reported in the banking sector, where digital banks employed credit scoring algorithms without ensuring adequate protection of customer personal data, allowing unauthorized access to confidential banking information (Poeta, 2020).

The impacts of the misuse of personal data by AI are multiple and can affect data subjects in different areas. In terms of fundamental rights, privacy violations can lead to algorithmic discrimination, where certain social groups are excluded or harmed based on biases embedded in AI systems (Caracas Bandeira & Ferreira, 2024). In the economic sphere, banking fraud and unauthorized transactions have been facilitated by the improper use of AI in recognizing financial patterns, as seen in Special Appeal No. 2.082.281-SP, judged by the Superior Court of Justice (STJ) in 2023, in which a bank was held liable for allowing fraudulent operations carried out by AI after the theft of a cellphone linked to a bank account (Brazil, 2023b).

Brazilian higher courts have faced challenges in interpreting and applying the LGPD in the context of AI, especially regarding the attribution of liability to companies. In the judgment of Special Appeal No. 2.130.619, the STJ reaffirmed the need for data controllers and processors to adopt effective preventive measures to avoid security incidents, under penalty of being held strictly liable for damages arising from failures in personal data processing (Brazil, 2024). This understanding reinforces the requirement of compliance with the LGPD, demanding that companies using AI demonstrate accountability and data governance, ensuring their practices align with regulatory requirements (Freire de Sá & Macena de Lima, 2021).

In the labor sphere, the use of AI in recruitment and performance management has been questioned regarding its compliance with labor rights and data protection. In a 2023 decision, the Superior Labor Court (TST) recognized the nullity of

an automated dismissal carried out by an AI system that classified employees as "low performance" without transparency regarding the criteria adopted (Araújo, 2022). This decision highlights the need for companies employing AI in human resource management to ensure that systems are aligned with the principles of transparency and non-discrimination, as required by the LGPD.

The case of the Paraná Court of Justice (TJPR), in Case No. 0018165-45.2022.8.16.0021, exemplifies the complexity of holding companies liable in cases of alleged data breaches. In this judgment, the plaintiff claimed that their personal data had been used to contract a phone line without consent, resulting in bank account blocks and financial fraud. However, the absence of material proof of the leak and the causal link between the company's conduct and the alleged damages led to the dismissal of the claim for compensation (Brazil, 2023a). The decision highlights the difficulty of establishing liability in cases where damages stem from AI system failures, especially when there is insufficient transparency about data flows.

In this scenario, it becomes evident that the use of AI in personal data processing requires robust governance mechanisms that ensure algorithmic decision traceability and allow the identification of potential violations. The National Data Protection Authority (ANPD) plays an essential role in defining minimum standards for AI use, as evidenced by Decision No. 11/2024/DIR-MW/CD, in which the entity reinforced the need for Data Protection Impact Assessments (DPIA) for all AI systems that perform automated decisions about individuals (ANPD, 2024). The absence of specific regulations for AI in Brazil creates legal gaps that can hinder corporate liability and compromise the effectiveness of data subject protection.

3. Identification of Legal Issues

The advancement of Artificial Intelligence (AI) in the processing of personal data imposes increasingly complex regulatory challenges, particularly concerning the compatibility of this technology with the fundamental principles of the Brazilian General Data Protection Law (LGPD-Law No. 13.709/2018). The LGPD establishes a normative framework focused on protecting privacy and the informational self-determination of data subjects, requiring companies to rigorously comply with the principles of purpose, necessity, transparency, security, and accountability (Lima & Sá, 2020). However, the growing sophistication of AI and its use in massive personal data processing raises questions about the effectiveness of current regulations and the legal system's ability to adapt to this new technological scenario.

The principle of purpose requires that data processing be carried out for legitimate, specific purposes informed to the data subject, without the possibility of further processing incompatible with the originally declared objectives, as established by Article 6 of the LGPD. This principle aims to ensure that the collection and use of personal information occur within a predetermined scope, preventing arbitrary or exploitative uses by organizations. It is also directly related to trans-

parency and the protection of individuals' privacy, ensuring that data is not manipulated in an excessive or disproportionate manner against the interests of the data subject.

> Article 6—Data processing activities must observe good faith and the following principles:
> I—purpose: processing for legitimate, specific, explicit, and informed purposes, with no possibility of further processing in an incompatible manner with these purposes;
> II—adequacy: compatibility of processing with the purposes informed to the data subject, according to the context of the processing;
> III—necessity: limitation of processing to the minimum necessary for the achievement of its purposes, with processing restricted to relevant, proportional, and non-excessive data in relation to processing purposes;
> IV—free access: guarantee to data subjects of facilitated and free consultation on the form and duration of processing, as well as on the entirety of their personal data;
> V—data quality: guarantee to data subjects of accuracy, clarity, relevance, and updating of data, according to necessity and for fulfilling the purposes of its processing;
> VI—transparency: guarantee to data subjects of clear, precise, and easily accessible information on data processing and the respective processing agents, while observing trade and industrial secrets;
> VII—security: use of technical and administrative measures capable of protecting personal data from unauthorized access and from accidental or unlawful situations of destruction, loss, alteration, communication, or dissemination;
> VIII—prevention: adoption of measures to prevent damages arising from personal data processing;
> IX—non-discrimination: impossibility of processing for illicit or abusive discriminatory purposes;
> X—accountability: demonstration by the agent of the adoption of effective measures capable of proving compliance with data protection rules and the effectiveness of such measures. (Brazil, 2018, Law No. 13.709).

In the context of AI, the principle of purpose faces significant challenges, since machine learning systems may identify patterns and make inferences that were not originally foreseen. As Caracas Bandeira and Ferreira (2024) point out, there is a regulatory gap regarding the use of data for algorithm training, especially when there is the possibility of secondary processing without the explicit consent of the data subject. This may compromise informational self-determination and transparency in data processing, in addition to heightening risks such as algorithmic discrimination and sensitive data leaks.

The principle of necessity requires that data processing be limited to the mini-

mum necessary for achieving its purpose (Brazil, 2018, art. 6, III). However, AI systems frequently require large volumes of data to ensure accuracy and efficiency, which may conflict with this principle. Studies such as those by Freire de Sá and Macena de Lima (2021) show that the use of AI in automated data processing often results in excessive data collection and prolonged storage, which may constitute an LGPD violation. This issue is worsened by the absence of clear normative guidelines regarding quantitative and temporal limits for algorithmic processing.

The principle of transparency requires that data subjects be clearly, accessibly, and ostensibly informed about how their data is being processed (Brazil, 2018, art. 6, VI). However, in the case of AI, a recurring issue is algorithmic opacity, known as "black boxes" (Poeta, 2020). This phenomenon occurs when decisions made by AI systems become incomprehensible even to their developers, preventing full observance of the transparency principle. This undermines the right to an explanation of automated decisions, as provided in Article 20 of the LGPD.

The principle of security is another essential guideline, requiring data controllers to adopt technical and administrative measures to protect data against unauthorized access, leaks, and security incidents (Brazil, 2018, art. 6, VII). Recent data leaks, such as those analyzed by Fama (2024), show that many companies still neglect robust cybersecurity protocols, leaving sensitive data vulnerable. The problem worsens when AI is used in critical sectors such as healthcare and finance, where cyberattacks may have severe consequences on data subjects' rights.

Finally, the principle of accountability obliges companies to demonstrate compliance with the LGPD (Brazil, 2018, art. 6, X). In this regard, the National Data Protection Authority (ANPD) plays a fundamental role in monitoring and defining technical parameters for AI governance in Brazil. Decision No. 11/2024 by ANPD establishes preliminary guidelines on best practices for automated data processing, including periodic audits, algorithm explainability, and continuous AI system review. However, regulation remains incipient, and the lack of concrete standards undermines legal predictability.

Corporate liability for the misuse of AI in personal data processing is grounded in Articles 42 to 45 of the LGPD, which establish hypotheses for both strict and fault-based liability. Strict liability applies when there is a failure in data security or noncompliance with legal obligations, regardless of intent or fault. Fault-based liability, in turn, requires proof of negligence, recklessness, or malpractice in AI use, which can be technically challenging given the complexity of algorithmic systems (Ludgero, 2024). The absence of a specific regulatory framework for civil liability arising from automated decisions creates legal uncertainty and hinders damage redress.

Penalties provided for LGPD violations include warnings, data blocking and deletion, suspension of activities, and fines of up to 2% of the company's revenue, limited to R$50 million per violation (Brazil, 2018, art. 52). However, enforcement remains a challenge, particularly in cases of AI-related violations. As shown in

decisions by the Superior Court of Justice (STJ), the technical complexity of algorithms often makes it difficult to directly attribute liability to companies (Brazil, 2024). This situation highlights the need for clearer and more detailed regulation for AI system oversight in Brazil.

The Brazilian legal framework still faces gaps regarding AI regulation, particularly in distinguishing between the liability of the algorithm developer and the company that employs it. As Paulo and Jacobsen (2023) point out, there is a growing tension between data protection and technological innovation, requiring a balanced regulatory approach. One alternative would be the adoption of a specific regulatory framework for AI, inspired by the European Artificial Intelligence Act, which imposes risk classifications and obligations proportional to the social impact of the technology.

The regulation of Artificial Intelligence (AI) has become a global concern due to the ethical, legal, and social challenges its application may generate. In the United States, there is a debate about the appropriate timing for regulation, since premature standardization could hinder innovation, while the absence of rules could pose risks to society. The European Union has proposed an Artificial Intelligence Act, classifying AI applications according to their risk level and prohibiting practices such as mass facial recognition in public spaces. China, meanwhile, has developed ethical guidelines emphasizing the need for human control over automated decisions. In Brazil, the General Data Protection Law (LGPD-Law No. 13,709/2018) establishes fundamental requirements for the use of AI in the collection and processing of personal data, demanding greater transparency and accountability from companies. Additionally, ABNT has developed technical standards to standardize and guide the governance and responsible use of AI in the country, following international guidelines.

The National Data Protection Authority (ANPD) has played a key role in implementing the LGPD, issuing guidelines that directly impact AI governance. Harmonizing technological innovation with legal compliance still faces challenges, especially regarding algorithm explainability and accountability for automated decisions. Studies indicate the need for specific regulations for high-risk AI, strengthened compliance measures, and the adoption of algorithmic audits to mitigate risks. ABNT Technical Standards, such as NBR ISO/IEC 42001, which deals with AI system governance, are essential to ensure that companies and institutions use technology ethically and transparently. In this way, balancing innovation with the protection of fundamental rights requires more robust policies, regular audits, and an updated regulatory framework that keeps pace with the global evolution of AI.

In this context, it becomes evident that the current LGPD regulation, although fundamental, still requires improvements to address the reality of AI use in automated decision-making. Defining minimum standards for algorithm transparency and auditability is essential to ensure greater legal certainty and effective protection for data subjects (Xavier & Dantas, 2021). The lack of normative harmo-

nization and fragmented jurisprudence complicate the uniform application of the rules, making a more decisive action by the legislator and the ANPD imperative.

The regulation of AI has become a global concern due to the ethical, legal, and social challenges its application may generate. In the United States, there is debate about the appropriate timing for regulation, as premature rulemaking may hinder innovation, while the absence of rules may pose societal risks. The European Union has proposed an Artificial Intelligence Act, classifying AI applications according to risk levels and prohibiting practices such as mass facial recognition in public spaces. China, on the other hand, has developed ethical guidelines emphasizing the need for human oversight of automated decisions. In Brazil, the LGPD (Law No. 13.709/2018) sets fundamental requirements for the use of AI in personal data collection and processing, demanding greater transparency and corporate accountability. In addition, ABNT (Brazilian Association of Technical Standards) has developed technical standards to guide the governance and responsible use of AI in the country, following international guidelines.

The National Data Protection Authority (ANPD) has played a fundamental role in implementing the LGPD, issuing guidelines that directly impact AI governance. Harmonizing technological innovation with legal compliance still faces challenges, especially regarding algorithm explainability and liability for automated decisions. Studies point to the need for specific regulation for high-risk AI, strengthening compliance measures, and adopting algorithmic audits to mitigate risks. ABNT's Technical Standards, such as NBR ISO/IEC 42001, which addresses AI systems governance, are essential to ensure ethical and transparent technology use by companies and institutions. Thus, balancing innovation with the protection of fundamental rights requires more robust policies, regular audits, and an updated regulatory framework that keeps pace with AI's global evolution.

In this context, it becomes clear that while the LGPD is essential, it still requires improvements to effectively address the reality of AI in automated decision-making. Defining minimum standards of algorithm transparency and auditability is crucial to ensuring greater legal certainty and effective protection of data subjects (Xavier & Dantas, 2021). The lack of normative harmonization and fragmented jurisprudence hinder uniform application of the law, making it imperative for the legislature and ANPD to adopt a more proactive stance.

4. Legal Analysis

The application of the General Data Protection Law (LGPD-Law No. 13,709/2018) in the processing of data through Artificial Intelligence (AI) requires an interpretative approach that balances the fundamental principles of data protection with the technological challenges posed by algorithmic systems. The increasing autonomy of solutions based on machine learning and deep learning generates complex legal implications, particularly regarding the responsibility of data controllers, the transparency of automated decision-making processes, and the mitigation of privacy and information security risks. In this context, an in-depth analysis of the

current regulatory framework and the doctrinal guidelines governing its application becomes essential (Ludgero, 2024).

A principles-based interpretation of the LGPD must take into account the foundations established in Article 6, which outlines parameters such as purpose, necessity, transparency, security, and accountability. Regarding transparency, the law requires that data subjects be informed about the criteria used in automated decision-making (Art. 20), ensuring their right to request detailed information about algorithmic processes affecting their legal sphere. However, as noted by Freire de Sá and Macena de Lima (2021), AI systems often operate through opaque architectures, hindering explainability and consequently compromising the protection of fundamental rights. This issue raises questions about the effectiveness of existing regulatory mechanisms and the need for specific regulation concerning the use of AI in personal data processing.

Civil liability for companies for the misuse of AI is supported by Article 42 of the LGPD, which establishes the responsibility of controllers and operators for potential property, moral, individual, or collective damages resulting from the irregular processing of personal information. Doctrine is divided regarding the applicable liability regime, with proponents of both strict liability, based on activity risk and the theory of internal fortuity, and subjective liability, dependent on proof of intent or fault in adopting inadequate security and regulatory compliance practices (Silva, 2023a). The prevailing view, however, converges toward a hybrid model, where strict liability applies to structural failures and subjective liability applies in cases demonstrating negligence in adhering to data governance guidelines.

Information security is a cornerstone of the LGPD and a central element in analyzing the law's applicability to AI systems. Article 46 requires data controllers to implement effective technical and administrative measures to ensure the integrity, confidentiality, and resilience of personal data. In this regard, Data Protection Impact Assessments (DPIAs), as provided in Article 38, are particularly relevant for evaluating risks associated with AI use, enabling early identification of potential vulnerabilities in automated processes. According to Poeta (2020), the absence of a specific legal requirement mandating DPIAs for all AI applications represents a significant regulatory gap, undermining the effectiveness of data subject protection.

From a jurisprudential perspective, recent decisions by the Superior Court of Justice (STJ) and the Superior Labor Court (TST) consolidate the trend of expanding corporate responsibility in data protection. In Special Appeal No. 2.082.281-SP (STJ, 2023), the STJ reaffirmed the duty of financial institutions to adopt robust fraud prevention mechanisms, recognizing their liability for illicit transactions resulting from the misuse of AI in banking systems. Similarly, labor jurisprudence has recognized the need for greater scrutiny of automated decisions in recruitment processes, considering that the use of AI without objective and transparent criteria may constitute a violation of the principle of equality and lead to algorithmic discrimination (Araújo, 2022).

The ethical dimension of AI must also be considered in interpreting the LGPD. Technological advances pose unprecedented challenges to data protection law, requiring the adoption of guidelines that ensure algorithmic neutrality and the prevention of discriminatory biases. As argued by Kaufman (2022) and Russell (2021), AI should be developed under a governance model that prioritizes fairness, transparency, and continuous human oversight. The implementation of codes of conduct and corporate best practices can help mitigate risks associated with data misuse, aligning regulatory compliance with contemporary ethical requirements.

The governance and compliance obligations imposed by the LGPD require companies to adopt a robust normative and operational framework, incorporating continuous monitoring mechanisms for their algorithmic operations. Measures such as the appointment of a Data Protection Officer (DPO), conducting internal audits, and creating transparent privacy policies are essential to ensure compliance with current legislation (Fama, 2024). Additionally, the adoption of algorithmic explainability technologies can aid in accountability and demonstrate adherence to legal obligations, reducing companies' exposure to administrative sanctions and lawsuits.

The existing regulatory gap in Brazil regarding AI highlights the need for more decisive action by the National Data Protection Authority (ANPD). Although the LGPD provides general guidelines for personal data processing, the absence of specific regulations for high-risk AI undermines legal certainty and complicates the oversight of abusive practices. Paulo and Jacobsen (2023) argue that adopting a dedicated AI regulatory framework, inspired by the European AI Regulation, could provide greater predictability and security for the sector, establishing differentiated levels of regulatory supervision according to the potential risk of the technological application.

The legal analysis of the LGPD's applicability to AI demonstrates that regulatory compliance must be treated as a strategic imperative for companies operating with automated data processing technologies. Implementing a structured governance system, conducting frequent audits, and investing in algorithmic oversight mechanisms are essential measures to ensure that AI is used ethically and in accordance with data protection principles. Moreover, harmonizing the LGPD with other sectoral legislation, such as the Consumer Protection Code, should be promoted to ensure a cohesive and effective legal model for privacy protection.

5. Practical Application

The application of the LGPD in the context of AI imposes substantial challenges on companies, which must adopt legal and operational mechanisms to ensure regulatory compliance and minimize liability risks arising from data breaches and misuse. The growing reliance on algorithms and automated systems for massive information processing requires the implementation of data governance strategies that guarantee compliance with the LGPD's fundamental principles, such as pur-

pose, necessity, transparency, security, and accountability (Fama, 2024). In this sense, corporate responsibility in using AI goes beyond mere regulatory compliance, demanding a commitment to effective privacy protection and mitigation of systemic risks.

Company liability for data breaches is primarily addressed through the sanctions provided in Articles 52 to 54 of the LGPD, which include warnings, fines of up to 2% of the company's revenue (limited to R$ 50 million per violation), suspension of database operations, and even prohibition of personal data processing (Silva, 2023b). Additionally, Article 42 establishes that the data controller or operator causing damage to a data subject must compensate for it, regardless of fault, if a violation of legal obligations is identified. This provision confirms the adoption of a hybrid liability regime, combining strict and subjective liability depending on the nature of the violation (Poeta, 2020).

Risk management in AI use must be a priority for companies, which need to adopt robust control mechanisms to prevent undue exposure of personal data. Key preventive measures include implementing a data governance program as recommended by Article 50 of the LGPD. Such a program should encompass continuous review of internal processes, adoption of technical security standards, and integration of best data protection practices, such as the privacy by design principle, which requires protective measures from the system design stage (Kaufman, 2022).

The appointment of a Data Protection Officer (DPO), as provided in Article 41, represents a key strategy to ensure regulatory compliance in AI use. The DPO acts as an intermediary between the company, data subjects, and the ANPD, advising the organization on best practices in personal data processing and ensuring internal processes comply with current legislation (Paulo & Jacobsen, 2023). Companies failing to appoint a responsible professional for data governance are more prone to compliance failures and, consequently, administrative sanctions and litigation.

Privacy and transparency policies also play a fundamental role in protecting data subjects and mitigating legal risks. According to Article 9 of the LGPD, controllers must provide clear and accessible information about data processing, including purpose, legal basis, and data subject rights. Lack of clarity in privacy policies may invalidate consent and violate the transparency principle, compromising the validity of data processing (Freire de Sá & Macena de Lima, 2021). Therefore, companies should adopt detailed terms of use specifying legal bases for processing and ensuring that data subjects understand how their information is used.

Conducting frequent audits and risk management is another essential measure to avoid LGPD violations in AI use. Article 46 imposes the duty to ensure data security against unauthorized access and incidents of undue exposure. Companies must implement cybersecurity protocols, perform vulnerability testing, and establish incident response plans to guarantee prompt detection and mitigation of any breach (Caracas Bandeira & Ferreira, 2024). Absence of effective internal controls

may constitute negligence in data protection, increasing corporate liability before the ANPD and judiciary.

Data Protection Impact Assessments (DPIAs), as provided in Article 38, are another key governance tool for mitigating risks in AI use. These reports must be prepared whenever data processing poses high risks to data subjects' fundamental rights, such as in automated decision-making, predictive analysis, and behavioral profiling systems. Failure to conduct a DPIA may be interpreted as violating the principle of prevention, increasing the company's exposure to administrative sanctions and lawsuits (Abrantes, 2023).

In addition to compliance measures, adopting ethical standards in AI use has become an increasing regulatory requirement worldwide. Implementing algorithmic ethics guidelines, as recommended by the European AI Regulation, represents an innovative approach to ensure automated systems are developed responsibly and respect data subjects' fundamental rights (Russell, 2021). Companies failing to integrate ethical principles into AI development risk severe reputational impacts and large-scale litigation.

Compliance with the LGPD requires organizations to adopt a proactive, multidisciplinary approach to personal data management. Combining structured governance, algorithmic oversight, and continuous monitoring is crucial to ensure AI use is transparent, secure, and compliant with regulatory guidelines (Lima & Sá, 2020). In this context, companies should invest in employee training to ensure all sectors understand the importance of data protection and act in accordance with applicable regulations.

The interaction between the LGPD and other sectoral regulations, such as the Consumer Protection Code (CDC), reinforces the need for an integrated approach to personal data protection. Applying consumer civil liability theory in the context of AI use expands corporate liability scenarios, requiring high levels of diligence and transparency in handling consumer information (Brazil, 1990). Noncompliance with LGPD guidelines may not only result in administrative penalties but also lead to compensation claims under consumer law.

In the labor context, using AI for recruitment and personnel management poses additional challenges. The Superior Labor Court (TST) has consolidated the understanding that automated decisions cannot result in discrimination or unequal treatment, under penalty of violating the principle of equality (Araújo, 2022). Therefore, companies using AI for resume analysis or performance evaluation must ensure employed algorithms are auditable, explainable, and free from discriminatory biases.

The need for specific AI regulation in Brazil has been debated among experts and legislators. Creating a dedicated AI regulatory framework, inspired by international models, could provide greater predictability and legal certainty for companies, establishing objective criteria to assess risks associated with AI use (Paulo & Jacobsen, 2023). The absence of specific regulation complicates ANPD oversight and increases legal uncertainty regarding corporate responsibility in AI use.

AI regulation in Brazil must consider the intersection of the LGPD and the need for more stringent governance mechanisms. The ANPD has played a crucial role in monitoring AI use to prevent privacy breaches and sensitive information leaks. However, experts point out that current legislation is not fully adapted to AI challenges, particularly regarding transparency and corporate accountability. The European General Data Protection Regulation (GDPR) is considered a robust model, providing clear guidelines for algorithmic explainability and protection of data subjects against automated financial decisions (European Union, 2016). In line with this trend, initiatives such as ABNT's NBR ISO/IEC 42001:2023 emerge as alternatives to standardize AI governance best practices and mitigate legal risks (ABNT, 2023).

In the United States, although no federal data protection law exists, state laws such as the California Consumer Privacy Act (CCPA) provide citizens with greater control over their information, requiring companies to provide transparency regarding personal data collection and use (CCPA, 2018). In Brazil, the LGPD provides similar measures, obliging controllers to allow data subjects access to, correction of, and, if necessary, deletion of their data (Brazil, 2018). However, experts argue that Brazil needs to advance in AI regulation, particularly in sectors like healthcare, finance, and recruitment, where automated decisions can directly impact individual rights. The OECD also recommends that countries adopt clear guidelines on ethical AI use, ensuring the technology is applied responsibly and without discrimination (OECD, 2013).

Compliance with the LGPD requires organizations to implement internal data governance programs, frequent audits, and algorithmic oversight to mitigate information leakage risks. Article 46 of Brazilian law mandates that controllers adopt security measures to protect data from unauthorized access, a recommendation also present in ISO/IEC 42001 (ABNT, 2023). Companies failing to invest in compliance mechanisms are subject to ANPD administrative evaluations and potential lawsuits under the Consumer Protection Code (Brazil, 1990).

The absence of specific AI regulation in Brazil forces courts such as the Superior Court of Justice (STJ) and the Federal Supreme Court (STF) to fill gaps with case-by-case decisions, generating legal uncertainty. The LGPD provides general guidelines for data processing but does not detail responsibility in automated decision-making cases, requiring judicial interpretation to define limits and obligations (Fama, 2024). This reliance on isolated decisions creates discrepancies in law enforcement and complicates standardization of best practices, exposing companies and citizens to legal and operational risks (Ludgero, 2024).

Without a dedicated AI regulatory framework, the ANPD's role in supervising and regulating algorithmic use is limited, leaving gaps in transparency, explainability, and automated system audits. This scenario fosters excessive litigation and reactive measures rather than preventive, efficient governance. Creating specific AI regulations would bring greater predictability and legal certainty, reducing reliance on isolated court decisions to define responsibilities and ethical boundaries

in technology application (Freire de Sá & Macena de Lima, 2021).

6. Conclusion with Recommendations and Final Considerations

The use of artificial intelligence in personal data processing represents one of the greatest contemporary legal challenges, requiring a balance between technological innovation and the protection of fundamental rights. The LGPD provides an essential normative framework to ensure that data processing activities are conducted transparently, securely, and ethically. However, the growing complexity of algorithmic systems and AI's decision-making autonomy generate regulatory gaps that hinder effective legislation enforcement, particularly regarding corporate liability and mitigation of risks associated with data leaks and misuse.

In this context, it is imperative that companies adopt robust compliance measures aligned with data governance principles and LGPD requirements. Implementing regular audits, conducting Data Protection Impact Assessments, and adopting algorithmic oversight mechanisms are essential to ensure regulatory compliance and minimize legal risks. Furthermore, transparency in AI use, through algorithm explainability and accountability to data subjects, must be a non-negotiable commitment to prevent reputational harm and large-scale litigation.

The ANPD also plays a fundamental role in establishing specific guidelines for AI use, setting minimum standards for security, ethics, and transparency in personal data processing. The lack of detailed regulation for high-risk AI systems still generates legal uncertainties and may compromise oversight of abusive practices. Therefore, it is advisable to develop complementary regulations that more specifically address algorithm governance and the protection of data subjects in the context of automated decision-making.

The evolution of artificial intelligence requires a dynamic regulatory approach, capable of adapting to new technological realities without restricting innovation. Developing guidelines that balance the need for data protection with operational feasibility for companies is essential to ensure a safe and predictable legal environment. Accordingly, AI regulation should be strategically conducted, considering successful international models and promoting ongoing dialogue between the public and private sectors to enable the implementation of best practices in data processing.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

Abrantes, P. C. de (2023). *Challenges and Dilemmas of Personal Data Protection in the Era of Algorithmic Culture*. SciELO Preprints.

Araújo, A. R. de (2022). *The Use of Personal and Artificial Data in Labor Relations: Protection, Discrimination, Digital Violence, and Harassment* (448 p.). Ministério Público do Trabalho.

Associação Brasileira de Normas Técnicas (2023). *NBR ISO/IEC 42001:2023—Information Technology—Artificial Intelligence Management*. ABNT.

Autoridade Nacional de Proteção de Dados (2024). *Vote No. 11/2024/DIR-MW/CD. Case No. 00261.004509/2024-36. Rapporteur: Miriam Wimmer*. ANPD.

Brazil (1990). *Consumer Defense Code—Law No. 8.078*. https://www.gov.br/mj/pt-br/assuntos/seus-direitos/consumidor/Anexos/cdc-portugues-2013.pdf

Brazil (2018). *Law No. 13.709*. https://www.gov.br/anpd/pt-br/centrais-de-conteudo/outros-documentos-e-publicacoes-institucionais/lgpd-en-lei-no-13-709-capa.pdf

Brazil (2023a). *Court of Justice of Paraná State. 2nd Small Claims Recursal Panel. Unnamed Appeal. Case No. 0018165-45.2022.8.16.0021. Rapporteur: Irineu Stein Junior. Cascavel District*. https://portal.tjpr.jus.br/jurisprudencia/j/2100000025254851/Acórdão-0018165-45.2022.8.16.0021

Brazil (2023b). *Supreme Court of Justice. Special Appeal No. 2.082.281-SP (2023/0222455-3)*. https://www.conjur.com.br/wp-content/uploads/2023/12/Banco-responde-por-Pix-feito-apos-ser-informado-de-roubo-de-celular.pdf

Brazil (2024). *Special Appeal No. 2.130.619*. https://www.jusbrasil.com.br/jurisprudencia/stj/1780119718

California (2018). *California Consumer Privacy Act (CCPA)—Assembly Bill No. 375*. https://oag.ca.gov/privacy/ccpa

California Consumer Privacy Act (CCPA). 2018. https://oag.ca.gov/privacy/ccpa

Caracas Bandeira, A. L. T., & Ferreira, J. S. A. B. N. (2024). Artificial Intelligence and the General Data Protection Law. *Revista do Ministério Público do Estado de Goiás, 28*. https://esump.mpgo.mp.br/ojs/index.php/rmpgo/article/view/27/10

Costa, A. A., & Bruno, D. R. (2025). AI-Artificial Intelligence: Impacts, Risks, and Benefits Challenging Modern Society. *Revista Interface Tecnológica, 1,* 76-87.

European Union (2016). *Regulation (EU) 2016/679*. General Data Protection Regulation. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679

Fama, J. S. (2024). Artificial Intelligence and Privacy: Legal and Ethical Implications in the Digital Era. *Revista Científica Multidisciplinar Núcleo do Conhecimento, 1,* 15-39. https://doi.org/10.32749/nucleodoconhecimento.com.br/tecnologia/implicacoes-legais

Freire de Sá, M. de F., & Macena de Lima, T. M. (2021). Artificial Intelligence and the General Data Protection Law: The Right to Explanation in Automated Decisions. *Revista Brasileira de Direito Civil, 4,* 227.

Kaufman, D. (2022). *Demystifying Artificial Intelligence* (331 p.). Autêntica.

Lima, T. M. M. de, & Sá, M. de F. F. de (2020). *Artificial Intelligence and the General Data Protection Law: The Right to Explanation in Automated Decisions* (pp. 227-246). Revista Brasileira de Direito Civil—RBDCivil, Belo Horizonte.

Ludgero, P. R. (2024). *Civil Liability for the Misuse of Artificial Intelligence in Candidate Selection Processes: Legal Implications in Brazil*. Jusbrasil.

Organization for Economic Cooperation and Development (OECD) (2013). *Privacy Principles and Personal Data Protection*.

Paulo, M. A., & Jacobsen, G. (2023). Challenges to the General Data Protection Law in the Era of Artificial Intelligence: Between the Right to Privacy and Robocalls. *Revista de*

Direito, Inovação, Propriedade Intelectual e Concorrência, Florianópolis, Brazil, 2.

Poeta, V. S. (2020). *Artificial Intelligence and Personal Data Protection: Effects of the European General Data Protection Regulation (GDPR) on Fundamental Rights Guarantees under Brazilian Law*. Master's Dissertation, Universidade do Vale do Itajaí.

Russell, S. (2021). *Artificial Intelligence in Our Favor: How to Maintain Control over Technology* (Trans. Berilo Vargas). Cia das Letras.

Sichman, J. S. (2021). Artificial Intelligence and Society: Advances and Risks. *Estudos Avançados, 35,* 37-50. https://doi.org/10.1590/s0103-4014.2021.35101.004

Silva, F. C. (2023b). *Protection of Sensitive Data in the Era of Artificial Intelligence*. Course Completion Work (MBA in Artificial Intelligence and Big Data), University of São Paulo.

Silva, P. R. A. da (2023a). *Civil Liability for Acts of Artificial Intelligence (AI): Regulatory Perspectives and the Relevance of ANPD's Role in Preventing Risks in Auto-Mated Data Processing*. Jusbrasil.

Superior Court of Justice (STJ) (2023). *Missed Opportunities, Possible Remedies: The Lost Chance Theory at the STJ*.

Veja (2025). *Largest Data Breach in Pix History Exposes Data from More than 11 Million Keys*. Veja. https://veja.abril.com.br/economia/maior-vazamento-da-historia-do-pix-expoe-dados-de-mais-de-11-milhoes-de-chaves/

Wang, S., Li, Y., Zhao, A., & Wang, Q. (2021). Privacy Protection in Federated Learning Based on Differential Privacy and Mutual Information. In *2021 3rd International Conference on Artificial Intelligence and Advanced Manufacture* (pp. 428-435). ACM. https://doi.org/10.1145/3495018.3495093

Xavier, M. R. P., & Dantas, A. G. A. (2021). Algorithmic Surveillance Device: Tracking Algorithms and Data Collection. *Simbiótica. Revista Eletrônica, 8,* 94-127. https://doi.org/10.47456/simbitica.v8i4.37348