Journal on Interactive Systems, 2026, 17:1
ISSN: 2763-7719 • doi: 10.5753/jis.2026.7128

Research Paper

Bridging Data Protection and AI Ethics: A Two-Study Empirical Examination of LGPD Principles and Ethical AI in Brazil

Ana Caroline da Rocha Braz [University of Brasília (UnB) | *anacarolinebraz26@gmail.com*]
João Rossi [University of Brasília (UnB) | *joaorossiborba@gmail.com*]
Edna Dias Canedo [University of Brasília (UnB) | *ednacanedo@unb.br*]

University of Brasilia (UnB), Department of Computer Science, Darcy Ribeiro University Campus, s/n, Asa Norte, Brasília, DF, 70910-900, Brazil.

Abstract. *Context:* Data protection laws and AI ethics frameworks are increasingly invoked to govern the risks of data-driven and algorithmic systems, but there is still limited empirical evidence on how practitioners and students perceive the relationship between legal principles (such as the Brazilian LGPD) and ethical principles for Artificial Intelligence (AI). *Goal:* This study investigates how LGPD principles are interpreted as a foundation for ethical AI, examining perceived alignments, practical challenges, regulatory gaps, and expectations for the evolution of AI governance in Brazil. *Method:* We conducted two complementary survey based studies. Study 1 collected responses from 30 computing students, exploring their perceptions of privacy, transparency, security, data minimization, and accountability in AI systems. Study 2 extended this investigation with 100 participants (students and professionals in diverse software project roles), using paired LGPD AI items, Likert-scale questions on sufficiency and complementarity, and open-ended questions analyzed through inductive content analysis. *Results:* Across both studies, participants consistently perceived strong conceptual alignment between LGPD principles and AI ethical principles, especially regarding privacy, transparency, security, prevention, non-discrimination, and accountability. However, they also reported important gaps, particularly in explainability, fairness and bias mitigation, inclusion and diversity, solidarity, and other human-centered values, as well as uncertainty about accountability for automated decisions and the fit of static legal principles to dynamic AI systems. *Conclusion:* The findings indicate that LGPD is viewed as a solid but insufficient foundation for ethical AI. Participants expect LGPD to be complemented or updated by AI specific ethical and regulatory frameworks, governance mechanisms, and technical measures such as explainable AI and algorithmic auditing, pointing to the need for an integrated ecosystem for responsible AI in Brazil.

Keywords: LGPD, Artificial Intelligence, Ethics, Data Protection, Responsible AI Governance.

Edited by: Darlinton Carvalho | **Received:** 07 December 2025 • **Accepted:** 04 March 2026 • **Published:** 13 March 2026

1 Introduction

Ethics, as a branch of philosophy, is concerned with the study of principles that guide human behavior, distinguishing between right and wrong, and justice and injustice. Rooted in the Greek term *ethos*, meaning character or custom, ethics explores issues related to morality, responsibility, and the values that underpin individual and collective actions (Wohlin *et al*., 2012). In contemporary technological contexts, ethical considerations have become increasingly essential, particularly in areas involving autonomy, large scale data processing, and decision-making systems.

Artificial Intelligence (AI) is a field within computer science focused on developing systems capable of performing tasks that typically require human intelligence, such as learning, classification, prediction, reasoning, and interaction with the environment or operating on data at a scale far beyond human analytical capacity (Russell *et al*., 1995; Finocchiaro, 2024). As a transformative technology, AI permeates domains such as health, education, public administration, cybersecurity, and the economy. However, the massive use of personal data, the opacity of many machine learning and generative models, and the delegation of consequential decisions to automated systems introduce complex ethical risks (Floridi *et al*., 2021; Maturo *et al*., 2025; Falcão and Canedo, 2024). These concerns include privacy breaches, discrimination, opacity, manipulation, and uncertain accountability (Jobin *et al*., 2019; Carvalho *et al*., 2025; Falcão and Canedo, 2024; McGrath *et al*., 2025), reinforcing the need to align AI development with established ethical and regulatory frameworks (Carrasco, 2025).

In Brazil, the General Data Protection Law (LGPD) represents the primary legal instrument governing personal data processing (Rocha *et al*., 2023). Although originally designed for traditional data-intensive systems, the LGPD establishes principles such as purpose limitation, adequacy, necessity, transparency, security, prevention, non-discrimination, and accountability, which are also central in frameworks for ethical AI (de Cerqueira *et al*., 2021). Recent empirical studies highlight that AI practitioners tend to more easily recognize technical principles (e.g., privacy, security, reliability) while showing less maturity concerning socio-ethical principles such as fairness, inclusion, and human well-being (Guimarães *et al*., 2025). Such asymmetries reinforce the importance of examining whether the LGPD can serve as an effective foundation for the ethical governance of AI. This article is an extended version of our earlier study (Braz and Canedo, 2025), substantially expanding the

data, analysis, and theoretical integration.

Motivated by these challenges, this research examines the relationship between LGPD principles and AI ethical principles through two complementary empirical studies. Study 1 collected responses from 30 computing students to analyze their perceptions of privacy, transparency, security, accountability, and other ethical dimensions in AI systems. Study 2 expanded this investigation by surveying 100 computing students and professionals across multiple roles in the software development lifecycle, providing a more diverse and mature perspective on the intersections between data protection and AI ethics. The studies combined quantitative analysis (Likert scale questions on principle alignment and sufficiency) with qualitative thematic analysis (open-ended reflections on legal adequacy, regulatory gaps, and expectations for the evolution of AI governance).

Our main findings reveal that participants consistently perceive strong conceptual alignment between LGPD principles and AI ethical principles, particularly in privacy, transparency, security, prevention, non-discrimination, and accountability. However, they also identify important gaps: limitations of LGPD in addressing explainability, fairness, bias mitigation, and socio-ethical principles; uncertainty regarding accountability for automated decisions; and challenges in applying static legal principles to dynamic, evolving AI systems. Participants argue that although LGPD provides a solid foundation for responsible AI, it is insufficient on its own, highlighting the need for complementary AI-specific regulation, governance frameworks, and technical mechanisms such as explainable AI.

This article is structured as follows: Section 2 presents the related work. Section 3 describes the research methodology. Sections 4 and 5 present the results of the two empirical studies. Section 6 synthesizes and compares the findings from Study 1 and Study 2. Section 7 discusses limitations and threats to validity. Finally, Section 8 provides the conclusion and outlines directions for future research.

2 Background and Related Works

2.1 Brazilian General Data Protection Law (LGPD)

On August 14, 2018, the Brazilian General Data Protection Law (LGPD), No. 13.709, was enacted by the President of the Republic. The LGPD aims to protect the fundamental rights of freedom, privacy, and the free development of each individual's personality (Macedo, 2018). It governs the processing of personal data, whether in physical or digital form, carried out by natural or legal persons under public or private law, and covers a wide range of operations performed through manual or digital means. In 2019, Law No. 13.853, approved on July 7, modified and added new elements to the LGPD. According to Article 2 of the LGPD (Macedo, 2018), the regulation of personal data protection is grounded in principles such as respect for privacy, informational self-determination, freedom of expression, inviolability of intimacy, technological development, free enterprise, and human dignity. Article 6 specifies the principles directly guiding the processing of personal data. Table 1 presents the LGPD principles (Rocha *et al*., 2023) considered in this study.

Under the LGPD, the processing of personal data may be performed by two types of agents: the **Controller**, responsible for decisions regarding the processing of personal data, and the **Processor**, who handles personal data on behalf of the controller. Additionally, the **Data Protection Officer (DPO)** serves as a communication channel between the controller, data subjects, and the National Data Protection Authority (ANPD) (Federal, 2021; Macedo, 2018; Martins *et al*., 2025; Spósito *et al*., 2025).

2.2 Ethical Principles in Artificial Intelligence

Artificial Intelligence (AI) aims to develop systems capable of performing tasks that typically require human intelligence, such as learning, reasoning, and decision-making. These systems rely on advanced algorithms that process large datasets to identify patterns, make autonomous decisions, generate recommendations, or interact with users through natural language (Russell *et al*., 1995; Finocchiaro, 2024; Danilevskyi *et al*., 2025).

AI has transformed multiple domains including healthcare, education, industry, and public administration bringing both opportunities and substantial ethical challenges (de Cerqueira *et al*., 2021; Machado *et al*., 2025). As AI systems become increasingly embedded in interactive technologies, ethical principles such as transparency, privacy, fairness, non-maleficence, accountability, human oversight, security, and equitable distribution of benefits have gained international recognition (UNESCO, 2022; Díaz-Rodríguez *et al*., 2023; de Cerqueira *et al*., 2021; Khan *et al*., 2022; Floridi *et al*., 2021; Jobin *et al*., 2019; González *et al*., 2024).

2.3 Related Works

Several studies have examined the intersection of ethics, artificial intelligence, and the LGPD, highlighting both conceptual and practical challenges. Brey and Dainow (2023) proposed an Ethics by Design approach to incorporate principles such as transparency, accountability, and fairness into AI systems from the outset. Khan *et al*. (2023) investigated how practitioners and policymakers perceive ethical issues in AI, identifying the need for clearer regulations and mechanisms for human oversight.

de Cerqueira *et al*. (2022) introduced the RE4AI Ethical Guide, an interactive card-based tool designed to support the elicitation of ethical requirements in AI systems. Developed using Design Science Research, the guide organizes 26 cards around 11 ethical principles (as described by Ryan and Stahl (2021)) and provides guiding questions, explanations, and illustrative examples. Evaluations with students showed its effectiveness in increasing ethical awareness, supporting requirements analysis, and mitigating ethics washing.

Recent research has expanded this discussion to specific sectors. For instance, Nascimento *et al*. (2024) analyzed ethical and legal aspects of AI in medicine, while Neves (2023) mapped the use of AI in clinical settings with a focus on privacy and informed consent. From a legal standpoint, Fernandes and MEIRA (2023) examined how AI challenges traditional legal frameworks in Brazil. Studies such as de Oliveira

Table 1. Principles and Definitions (LGPD)

Principle	Definition
I - Purpose	Processing must be carried out for legitimate, specific, explicit, and informed purposes, and subsequent processing must not be incompatible with those purposes.
II - Adequacy	Processing must be compatible with the purposes informed to the data subject, according to the context of the processing.
III - Necessity	Processing must be limited to the minimum necessary to fulfill its purposes, covering only relevant, proportional, and non-excessive data.
IV - Free Access	Data subjects must be guaranteed easy and free access to information about the form and duration of processing, as well as to the completeness of their personal data.
V - Data Quality	Ensures data subjects the right to accurate, clear, relevant, and up-to-date data, according to the necessity and for the fulfillment of the purpose of the processing.
VI - Transparency	Data subjects must have clear, precise, and easily accessible information about the processing being carried out and the respective processing agents, subject to commercial and industrial secrecy.
VII - Security	The use of technical and administrative measures to protect personal data from unauthorized access and accidental or unlawful situations of destruction, loss, alteration, communication, or dissemination.
VIII - Prevention	Adoption of measures to prevent the occurrence of harm resulting from the processing of personal data.
IX - Non-discrimination	Data processing must not be carried out for discriminatory, unlawful, or abusive purposes.
X - Accountability	The controller or processor must demonstrate the adoption of effective measures capable of proving compliance with the law and the effectiveness of those measures.

(2024) and de Araújo Neto and Barbosa Aguiar (2024) contributed to understanding the enforcement of LGPD and its implications for information security practices. Other works, such as Rapôso *et al*. (2019) and Sarlet and Ruaro (2021), reviewed trends in the application of LGPD principles in technological contexts and highlighted gaps in developers' knowledge of privacy requirements. From a broader legal perspective, prior research has also examined specific implications of the LGPD in emerging digital contexts, such as the treatment of digital legacy and post-mortem data (Beppu *et al*., 2021). These studies demonstrate the expanding interpretative scope of the LGPD and illustrate how its principles continue to be tested in novel socio-technical scenarios, including those influenced by data-driven technologies.

Ethical challenges in AI development have also been explored in domains such as cybersecurity (González *et al*., 2024), content generation (Quintino *et al*., 2024), and computational social science (Carvalho *et al*., 2021). These studies emphasize the difficulty of ensuring transparency, fairness, and accountability within algorithmic systems, especially when processing personal data or making automated decisions.

Challenges in Operationalizing Ethical Principles in AI Development. Pant *et al*. (2025) investigated how AI developers understand and address fairness in real-world software projects. Their grounded theory analysis revealed that practitioners face substantial obstacles in translating abstract ethical principles such as fairness, accountability, and non-discrimination into concrete engineering practices. Key challenges include conflicting metrics for fairness, insufficient resources, limited organizational support, and uncertainty about how regulatory or ethical guidelines should be applied in the development lifecycle. These findings align with previous literature suggesting that ethics in AI often remains aspirational rather than actionable, reinforcing the need for frameworks that bridge the gap between high-level principles and practical implementation.

Guimarães *et al*. (2025) investigated how Brazilian software developers working in AI teams perceive ethical principles and navigate dilemmas that emerge during the development of intelligent systems. Through a mixed-method study combining survey data and interviews, the authors found that professionals more readily recognize technical principles such as privacy, reliability, and security while demonstrating lower adherence to socio-ethical principles such as well-being, equity, and sustainability. The study also highlights structural barriers to the implementation of ethical practices, including pressure for rapid delivery, conflicts with commercial interests, lack of organizational governance, and hierarchical constraints that limit developers' agency. These findings converge with those of the present study, particularly regarding the difficulty of operationalizing ethical principles and the asymmetry between the maturity of LGPD technical principles and the more human-centered principles of AI ethics.

In the Brazilian context, Porto *et al*. (2025) conducted a Systematic Literature Review on ethical requirements in AI systems, identifying recurring principles such as fairness, transparency, accountability, and privacy, and examining how these principles are translated into requirements engineering practices. Their findings highlight the persistent gap between high-level ethical guidelines and their operationalization in software artifacts, reinforcing the need for structured approaches to elicit, formalize, and validate ethical requirements. While their study focuses on methodological strategies for embedding ethics into system design, it does not investigate how such principles are perceived in relation to national regulatory frameworks such as the LGPD. Our study complements this line of research by empirically examining how students and professionals conceptually relate legal data protection principles to AI ethical values.

Recent Evidence on Ethical Compliance Tools and Challenges. More recent literature has identified critical gaps in translating ethical principles into practical mechanisms for evaluating AI systems. The comprehensive review by Cappelli and Serugendo (2025) showed that existing tools for assessing AI ethics compliance are scarce and predominantly manual. Their analysis highlights the lack of auto-

mated or semi-automated methods, the diversity and inconsistency of ethical principles across organizations, and the challenges companies face in determining which regulatory or ethical guidelines to apply. These findings reinforce the need for structured models and tools capable of supporting both ethics-by-design and post-deployment audits. According to the authors, the difficulty in operationalizing principles such as transparency, fairness, safety, and accountability represents a major barrier to trustworthy AI.

Evidence on Ethics Education and Awareness. Complementary to the compliance perspective, Kipman *et al*. (2025) investigated students' perceptions of ethical principles in AI and found that many computing students feel unprepared to apply ethical concepts in real development scenarios. Their work highlights the gap between theoretical exposure and practical competence, an issue directly relevant to the perceptions captured in our survey. This reinforces the importance of investigating how future developers interpret the relationship between LGPD principles and AI ethics.

Complementing this perspective, recent Brazilian research has investigated how organizational leaders perceive trust and governance in AI systems. The study by Gonçalves *et al*. (2024), conducted with C-Level executives, indicates that trust in AI adoption is strongly associated with regulatory clarity, transparency mechanisms, and accountability structures. Although focused on executive decision-making rather than technical development, their findings reinforce the centrality of regulatory and ethical alignment in shaping professional and organizational attitudes toward AI.

Together, the literature reveals a consistent challenge: although AI ethics frameworks and data protection laws such as the LGPD provide a strong normative foundation, there remains limited empirical understanding of how these principles intersect in the perceptions of students and practitioners, and how they may be translated into actionable practices. This gap motivates the present study and underscores its relevance.

International Perspectives on AI Ethics Education and Regulatory Contexts. Recent international research has examined how ethical principles, data protection, and AI governance are addressed within computing and higher education contexts. A systematic review of ethics in computing education conducted by Brown *et al*. (2024) analyzed over one hundred ACM publications and identified significant heterogeneity in how ethical competencies are conceptualized, taught, and assessed. The authors emphasize that while ethical principles are increasingly present in curricula, there remains limited empirical evidence on how students interpret or internalize these principles in relation to real regulatory environments.

Similarly, large-scale European surveys on the teaching of computer ethics Stavrakakis *et al*. (2022) reveal substantial variation in institutional approaches, ranging from standalone ethics courses to embedded modules within technical disciplines. Although these studies discuss the role of frameworks such as the GDPR in shaping curricular content, they do not empirically examine how students and practitioners perceive the alignment between national data protection regulation and broader AI ethical principles.

More recently, empirical work on student perceptions of data governance and learning analytics in regulated contexts has emphasized concerns related to transparency, consent, and informational self-determination (Karimov *et al*., 2025). In parallel, policy-oriented analyses of ethical principles for AI in education (Nguyen *et al*., 2023) have mapped global governance guidelines proposed by organizations such as UNESCO and OECD. However, these studies predominantly focus on normative frameworks or educational design, rather than on how computing students and professionals conceptualize the relationship between domestic regulatory instruments and AI ethics in specific socio-legal contexts.

By contrast, the present study contributes empirical evidence from the Brazilian context, exploring how LGPD principles are interpreted in relation to AI ethical values by both students and practitioners. Rather than assessing regulatory compliance or technical implementation, this study focuses on regulatory perception as a socio-technical dimension of AI governance. This perspective complements international research on ethics education while foregrounding the interpretative dimension of regulation in emerging AI ecosystems.

3 Research Methodology

This research aims to investigate how the ethical principles of the Brazilian General Data Protection Law (LGPD) relate to ethical principles commonly adopted in Artificial Intelligence (AI), and how these principles are perceived by students and professionals in computing. The study was conducted in two phases: (1) an exploratory survey (Study 1), and (2) an extended and redesigned survey (Study 2), developed for this article.

To maintain methodological consistency with the original publication while enabling the expanded analysis, we keep the two original research questions and introduce two new research questions exclusively addressed by Study 2:

- **RQ1.** What are the main ethical principles found in both the LGPD and Artificial Intelligence, and how are they related?
- **RQ2.** What challenges arise in applying the ethical principles of the LGPD and Artificial Intelligence, and how can they be addressed?
- **RQ3.** How do computing students and professionals evaluate the degree of alignment between specific LGPD principles and AI ethical principles?
- **RQ4.** How do participants evaluate the sufficiency of LGPD principles for guiding ethical AI, what ethical gaps do they identify, and how do they expect the law to evolve in response to AI-related challenges?

We adopted a multi-method exploratory approach involving a literature review, document analysis, and two survey-based empirical studies. The literature review followed guidelines by Kitchenham and Charters (2007) and Petersen *et al*. (2008), and its findings guided the construction of both survey instruments.

3.1 Study 1: Survey Instrument and Participants

Study 1 consisted of a Google Forms questionnaire distributed to students in computing programs. It included demographic questions, self-assessment of familiarity with LGPD and AI principles, and Likert scale statements regarding privacy, transparency, data minimization, explainability, accountability, and other ethical values.

The complete list of questions from Survey 1 is presented in Table 2, including the mapping of each question to the research questions addressed in Study 1 (RQ1 and RQ2).

3.2 Study 2: Extended Survey Instrument and Participants

Study 2 expands Study 1 by including a more diverse population (students and professionals), a larger set of constructs, and explicit pairwise comparisons between LGPD principles and AI ethical principles. The instrument was validated through a pilot test with three professionals, after which minor linguistic adjustments were made.

Survey 2 contains four major sections: (1) demographic questions, (2) familiarity with LGPD and AI ethics, (3) direct comparisons between LGPD and AI principles, and (4) perceptions about regulatory sufficiency, gaps, and expectations for future updates. The complete list of questions appears in Table 3.

Data from both surveys were analyzed through a mixed-method strategy. Closed questions were interpreted using descriptive statistics, enabling comparisons between Study 1 and Study 2. Open-ended responses (Study 2) were examined using inductive content analysis, allowing themes to emerge regarding perceived gaps, regulatory needs, and expectations for future AI governance.

The triangulation between the two studies provides a richer understanding of the degree of alignment between LGPD and AI ethics (RQ1–RQ3) and offers insights into perceived regulatory gaps and expectations for future legal evolution (RQ4).

This study followed ethical procedures including voluntary participation, informed consent, and full anonymization of responses. No personally identifiable information was collected, and participants could withdraw at any time without penalty. In accordance with Brazilian Resolution CNS 510/2016, opinion-based surveys conducted without participant identification may be exempt from formal ethics committee review. As the study involved anonymous perception based responses without the collection of sensitive or identifiable data, it was conducted under this exemption framework.

Beyond procedural compliance, we recognize that ethical considerations extend to the interpretation and dissemination of findings. Given that a portion of the participants were students or early-career professionals, potential power asymmetries inherent to academic contexts must be acknowledged. To mitigate this risk, participation was entirely voluntary and responses were collected anonymously, without any academic or professional consequences. Furthermore, the findings reflect subjective perceptions within a specific socio-educational context and should not be interpreted as prescriptive guidance for regulatory reform or policy decisions. Rather, they contribute exploratory evidence regarding how regulatory and ethical principles are conceptually understood within the computing community.

4 Results — Study 1

The survey received 30 responses, with 60% from Computer Science students, 20% from Computer Science Education students, 10% from Computer Engineering students, and 10% from students enrolled in other programs. Regarding prior knowledge, only 36.7% reported being familiar with the principles of the LGPD, 43.3% stated they knew a little, and 20% indicated they were not familiar at all. Knowledge of AI ethical principles was even lower: only 16.7% claimed to know them, 33.3% reported knowing a little, and 50% stated they had no knowledge (Figure 1).

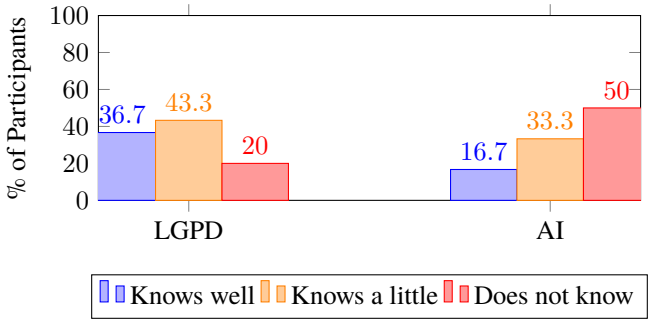

Figure 1. Participants' Knowledge of LGPD and AI Principles

4.1 RQ.1: What are the main ethical principles found in both the LGPD and Artificial Intelligence, and how are they related?

The results show that participants perceive a strong connection between LGPD principles and the ethical principles that guide responsible AI development. This alignment is particularly apparent in the domains of privacy, transparency, security, and data minimization. Participants P#3, P#9, P#18, and P#29 stated, respectively:

"Privacy: The protection of personal data should be considered equally important, both in corporate data collection and in the use of AI systems."

"Transparency: Companies and AI systems should be equally transparent regarding the use and sharing of personal data."

"Data Minimization and Security: In both LGPD and AI development, data minimization and security are necessary aspects for protecting individuals."

"Accountability: AI developers should be held accountable for the impacts of decisions made by AI systems."

Approximately 90% of the participants agreed that LGPD principles can serve as a foundation for ensuring that AI systems respect user privacy by establishing clear rules for data collection and processing. Transparency emerged as an equally important concern, with 90% of participants affirming that AI systems should incorporate explainability to ensure that automated decisions are understandable to users (Figure 2).

Table 2. Survey 1 Items and Corresponding Research Questions

ID	Question (Full Text in English)	Related RQ
Q1	Informed Consent Form (I agree / I do not agree)	–
Q2	What is your gender?	–
Q3	What is your academic program?	–
Q4	What is your age?	–
Q5	Do you know the principles of the LGPD? (Yes / No / A little)	RQ1
Q6	Do you know the ethical principles of Artificial Intelligence? (Yes / No / A little)	RQ1
Q7	"I believe that companies should be transparent about how my personal data is collected, processed, and stored." (Likert 1–5)	RQ1
Q8	"The security of my personal data is an important priority for the companies that collect it." (Likert 1–5)	RQ1
Q9	"It should be necessary to obtain my explicit consent before any organization collects and uses my personal data." (Likert 1–5)	RQ1
Q10	"It is important that I have the right to access, correct, or delete my personal data at any time." (Likert 1–5)	RQ1
Q11	"I believe that companies should collect only the data that is necessary for a specific purpose, avoiding excessive collection." (Likert 1–5)	RQ1
Q12	"I believe that the algorithms used in Artificial Intelligence should be explainable and understandable to users." (Likert 1–5)	RQ2
Q13	"AI developers should be responsible for the impacts of decisions made by AI systems." (Likert 1–5)	RQ2
Q14	"Users' privacy should be protected at all times when using Artificial Intelligence systems." (Likert 1–5)	RQ1
Q15	"AI systems should be designed to ensure that there is no discrimination against any group of people." (Likert 1–5)	RQ2
Q16	"The security of AI systems should be a priority to prevent harm or misuse of the technology." (Likert 1–5)	RQ2
Q17	"The protection of personal data should be considered equally important both in data collection by companies and in the use of AI systems." (Likert 1–5)	RQ1, RQ2
Q18	"Companies and AI systems should be equally transparent regarding the use and sharing of personal data." (Likert 1–5)	RQ1
Q19	"Both the LGPD and AI ethical principles should ensure that users have control over their data and automated decisions." (Likert 1–5)	RQ1
Q20	"In both the LGPD and AI development, data minimization and security are essential aspects for protecting individuals." (Likert 1–5)	RQ1
Q21	"The social and ethical impacts of technologies related to both data protection and artificial intelligence should be considered equally important." (Likert 1–5)	RQ2

In addition, 76.7% emphasized the importance of data minimization and security, core components of the LGPD, arguing that AI systems should avoid unnecessary data collection and implement strong safeguards to protect users' information. Information security was also highlighted as a shared concern across both domains, reinforcing the need for robust protection mechanisms for stored data and algorithmic decision-making processes.

Lastly, around 40% of participants agreed that AI developers should be accountable for decisions produced by automated systems, reflecting the LGPD's emphasis on accountability. These perceptions suggest that future AI regulations may benefit from adopting LGPD like governance structures, particularly regarding transparency, auditing, and compliance (Figure 2).

RQ.1 Summary: Participants associated LGPD principles with AI ethics, emphasizing privacy, transparency, data minimization, and accountability as the strongest points of convergence. Overall, they indicated that LGPD principles can help guide ethical AI development, especially regarding privacy, transparency, security, and data minimization.

4.2 RQ.2. What challenges arise in applying the ethical principles of the LGPD and Artificial Intelligence, and how can they be addressed?

Despite the conceptual alignment observed, participants identified several challenges associated with applying LGPD principles to AI systems. Explicit consent was strongly endorsed, with 86.7% agreeing that organizations should obtain explicit permission before collecting or using personal

Table 3. Survey 2 Items and Corresponding Research Questions

ID	Question (Full Text in English)	Related RQ
Q1	Informed Consent Form (I agree / I do not agree)	–
Q2	What is your gender?	–
Q3	What is your age?	–
Q4	What is your academic program?	–
Q5	Which role best describes your current activities in software projects?	–
Q6	How many years of experience do you have as a developer?	–
Q7	Do you know the principles of the LGPD? (Yes / No / A little)	RQ1
Q8	Do you know the ethical principles of Artificial Intelligence? (Yes / No / A little)	RQ1
Q9	LGPD's Purpose principle and the Beneficence principle of AI Ethics — How do these principles relate? (Likert 1–5)	RQ3
Q10	LGPD's Adequacy principle and the Fairness/Justice principle of AI Ethics — How do these principles relate? (Likert 1–5)	RQ3
Q11	LGPD's Necessity principle and the Non-maleficence principle of AI Ethics — How do these principles relate? (Likert 1–5)	RQ3
Q12	LGPD's Free Access principle and the Transparency principle of AI Ethics — How do these principles relate? (Likert 1–5)	RQ3
Q13	LGPD's Data Quality principle and the Explainability principle of AI Ethics — How do these principles relate? (Likert 1–5)	RQ3
Q14	LGPD's Transparency principle and the Responsibility/Accountability principle of AI Ethics — How do these principles relate? (Likert 1–5)	RQ3
Q15	LGPD's Security principle and the Privacy/Data Governance principles of AI Ethics — How do these principles relate? (Likert 1–5)	RQ3
Q16	LGPD's Prevention principle and the Robustness/Safety principle of AI Ethics — How do these principles relate? (Likert 1–5)	RQ3
Q17	LGPD's Non-discrimination principle and the Inclusion/Diversity principles of AI Ethics — How do these principles relate? (Likert 1–5)	RQ3
Q18	LGPD's Accountability principle and the Accountability principle in AI Ethics — How do these principles relate? (Likert 1–5)	RQ3
Q19	"The principles of the LGPD are sufficient to guide the ethical use of AI systems." (Likert 1–5)	RQ4
Q20	"The ethical principles of AI extend and complement those of the LGPD." (Likert 1–5)	RQ4
Q21	Which LGPD principle do you consider most relevant for ethical AI development? (Select all that apply)	RQ4
Q22	Which AI ethical principle do you believe is not covered by the LGPD? (Select all that apply)	RQ4
Q23	"Do you believe that AI ethical principles can serve as a basis for future revisions of the LGPD?" (Yes / No / Maybe)	RQ4
Q24	"Do you believe the LGPD should be updated to address ethical challenges related to AI? Please explain." (Open-ended response)	RQ4

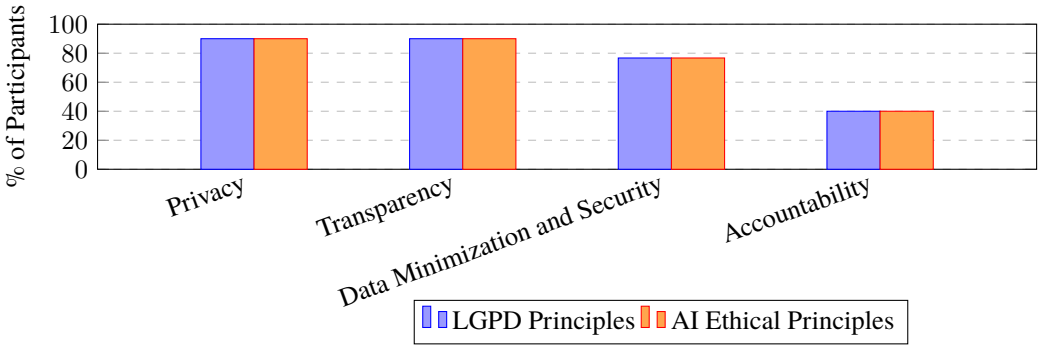

Figure 2. Participants' perceptions of alignment between LGPD principles and AI ethical principles.

data. However, AI systems often rely on continuous learning processes, making consent traceability and updates difficult. Participants pointed toward the need for *dynamic consent management* systems that enable users to review, modify, or withdraw their consent over time (Figure 3).

Regarding data security, 50% of respondents agreed that protecting personal data should be a high priority for companies using AI. Nevertheless, concerns were raised about enforcing this principle, given the increased volume and sensitivity of data used by AI algorithms. Strengthening

data protection measures such as encryption, anonymization, and strict access controls was highlighted as important.

Only 40% of respondents agreed that AI developers should be held accountable for outcomes produced by AI systems. This reflects broader societal uncertainty about responsibility when AI operates autonomously or through complex decision pipelines. Participants implicitly suggested the need for clearer legal frameworks to define liability in AI contexts.

Finally, only 43.3% agreed that AI algorithms should be explainable and understandable. Although this percentage is modest, it still indicates growing awareness of the importance of explainability in mitigating risks, improving trust, and supporting auditing processes.

RQ.2 Summary: Participants highlighted four main challenges: (1) obtaining and maintaining meaningful consent in dynamic AI systems, (2) ensuring security when processing large scale data, (3) assigning accountability for automated decisions, and (4) enabling sufficient algorithmic transparency. Suggested solutions include dynamic consent mechanisms, stronger cybersecurity practices, clearer legal responsibility frameworks, and investments in Explainable AI (XAI).

5 Results — Study 2

Study 2 collected 100 valid responses from students and professionals in Computing and related areas, recruited via social networks and professional contacts. All participants who agreed to the informed consent form were included in the analysis, and all data were treated in aggregate and anonymized form.

5.1 Participant Profile

Most respondents identified as men (75%), followed by women (24%) and 1% who preferred not to disclose their gender (Q2). The age distribution (Q3) was predominantly concentrated among young adults: the largest group was between 19 and 24 years old (45%), followed by participants in the ranges 46–50 years (17%), 25–30 years (10%), 41–45 years (10%), 36–40 years (9%), 31–35 years (7%), above 50 years (11%), and a small number under 18 (1%), as shown in Table 4. This distribution reflects a diverse mix of undergraduate students and experienced professionals.

Regarding academic background (Q4), the majority were enrolled in Computer Science (51%), followed by Software Engineering (18%), other Computing-related programs (20%), Information Systems (9%), and Computer Engineering (2%). This composition indicates that the sample is strongly aligned with computing education and practice.

In terms of professional roles (Q5) within software projects, participants most frequently identified as Software Developers (34%), followed by Systems Analysts (17%), Project Managers (14%), Software Engineers (12%), Data Scientists or Data Engineers (9%), Requirements Engineers (4%), Technical Leaders or Architects (4%), DevOps or Infrastructure Engineers (3%), and other technical roles (3%). These results show broad representation across the software development lifecycle.

Regarding experience as a developer (Q6), 41% reported having less than one year of experience, 26% indicated between 1 and 5 years, 10% between 6 and 10 years, 6% between 11 and 15 years, and 17% more than 15 years. Taken together, these results demonstrate a heterogeneous sample composed of early career practitioners and senior professionals, complementing Study 1, which consisted mainly of students.

Knowledge about LGPD (Q7) and AI ethical principles (Q8) was also higher than in Study 1. For LGPD principles, 63% stated they know them, 28% know a little, and 9% do not know them. For AI ethical principles, 43% reported knowing them, 35% know a little, and 22% do not know them (Table 4).

5.2 RQ3. How do computing students and professionals evaluate the degree of alignment between specific LGPD principles and AI ethical principles?

To examine how participants perceive the conceptual alignment between LGPD principles and AI ethical principles, Study 2 included ten paired items (Q9–Q18), each assessed on a five-point Likert scale. The results reveal a clear and consistent trend: in all principle pairs, the majority of participants selected high agreement levels (4 or 5), indicating that respondents perceive strong correspondence between data protection principles and ethical expectations for AI systems.

For the pair *Purpose (LGPD)* and *Beneficence (AI ethics)* (Q9), 79% of participants chose values 4 or 5, with responses distributed as follows: 1 (3%), 2 (2%), 3 (16%), 4 (44%), and 5 (35%), as shown in Figure 4. This suggests that respondents associate legitimate, well defined purposes in data processing with the ethical obligation of AI to promote human well-being.

A similar pattern emerged for *Adequacy (LGPD)* and *Justice and Equity (AI ethics)* (Q10). Most participants again selected high agreement levels, with 64% choosing values 4 or 5. The full distribution was: 1 (7%), 2 (5%), 3 (24%), 4 (34%), and 5 (30%). The results indicate that participants tend to link the contextual appropriateness of data use to fairness and equitable treatment in algorithmic outcomes.

In the third pair, *Necessity (LGPD)* and *Non-maleficence (AI ethics)* (Q11), 67% of respondents selected values 4 or 5. Responses were: 1 (4%), 2 (9%), 3 (20%), 4 (38%), and 5 (29%). These results suggest that limiting data collection to what is strictly necessary is perceived as a mechanism for minimizing potential harm produced by AI systems.

The pair *Free Access (LGPD)* and *Transparency (AI ethics)* (Q12) exhibited one of the strongest alignments, with 79% selecting 4 or 5. Responses were: 1 (2%), 2 (3%), 3 (16%), 4 (40%), and 5 (39%). Participants appear to interpret both principles as ensuring that individuals can understand and monitor how their data and automated decisions are handled.

For *Data Quality (LGPD)* and *Explainability (AI ethics)* (Q13), 73% of respondents chose 4 or 5. The distribution was: 1 (3%), 2 (4%), 3 (20%), 4 (46%), and 5 (27%). These results suggest that accurate and reliable data are seen as fun-

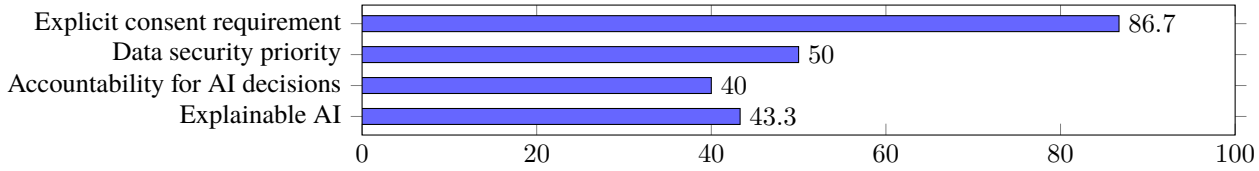

Figure 3. Participant agreement with key ethical principles and challenges in applying LGPD to AI (N=30).

Table 4. Demographic and professional profile of Study 2 participants ($n = 100$).

Gender	#	%
Male	75	75%
Female	24	24%
Prefer not to say / Other	1	1%
Age group	#	%
Under 18 years	1	1%
19–24 years	45	45%
25–30 years	10	10%
31–35 years	7	7%
36–40 years	9	9%
41–45 years	10	10%
46–50 years	17	17%
Above 50 years	11	11%
Academic Program	#	%
Computer Science	51	51%
Software Engineering	18	18%
Information Systems	9	9%
Computer Engineering	2	2%
Other Computing related program	20	20%
Role in Software Projects	#	%
Software Developer (backend / frontend / fullstack)	34	34%
Systems Analyst	17	17%
Project Manager	14	14%
Software Engineer	12	12%
Data Scientist / Data Engineer	9	9%
Requirements Engineer	4	4%
Technical Leader / Architect	4	4%
DevOps / Infrastructure Engineer	3	3%
Other role in software projects	3	3%
Experience as Developer	#	%
Less than 1 year	41	41%
1–5 years	26	26%
6–10 years	10	10%
11–15 years	6	6%
More than 15 years	17	17%
Knowledge of LGPD Principles	#	%
Knows	63	63%
Knows a little	28	28%
Does not know	9	9%
Knowledge of AI Ethical Principles	#	%
Knows	43	43%
Knows a little	35	35%
Does not know	22	22%

damental for AI systems to generate outputs that are interpretable and justifiable.

The pair *Transparency (LGPD)* and *Responsibility/Accountability (AI ethics)* (Q14) likewise showed strong agreement, with 74% selecting values 4 or 5. Responses were: 1 (4%), 2 (3%), 3 (19%), 4 (34%), and 5 (40%). This reflects the perception that transparent communication about data processing aligns closely with accountability in AI development and deployment.

The strongest alignment of all pairs occurred in *Secu-*

rity (LGPD) and *Privacy and Data Governance (AI ethics)* (Q15). In this case, 79% of participants selected high agreement levels (4 or 5), with 21% choosing 4 and 58% choosing 5. The full distribution was: 1 (2%), 2 (3%), 3 (16%), 4 (21%), and 5 (58%). This makes Q15 the pair with the clearest consensus that LGPD and AI ethics strongly reinforce each other regarding data protection and governance.

Similarly, *Prevention (LGPD)* and *Robustness and Safety (AI ethics)* (Q16) showed high agreement, with 76% selecting 4 or 5. Responses were: 1 (1%), 2 (5%), 3 (18%), 4 (31%), and 5 (45%). Participants appear to interpret preventive measures in data protection as a direct parallel to designing AI systems that avoid failure and resist adversarial conditions.

The pair *Non-discrimination (LGPD)* and *Inclusion and Diversity (AI ethics)* (Q17) also demonstrated strong perceived alignment, with 75% selecting 4 or 5. Distribution: 1 (3%), 2 (7%), 3 (15%), 4 (33%), and 5 (42%). This reflects widespread awareness of the risk of algorithmic bias and the importance of inclusive design.

Finally, *Accountability (LGPD)* and *Accountability (AI ethics)* (Q18) yielded another strong alignment, with 81% selecting 4 or 5. Responses were: 1 (1%), 2 (1%), 3 (17%), 4 (36%), and 5 (45%), as shown in Figure 4. This indicates strong participant consensus that the accountability mechanisms envisioned in LGPD are directly relevant to responsible AI development.

Taken together, the results of Q9–Q18 demonstrate that computing students and professionals perceive a substantial conceptual convergence between LGPD principles and AI ethical principles. High levels of agreement across all pairs indicate that participants view LGPD not only as a data protection framework but also as a foundational element for ethical AI governance. Moreover, the consistency of positive evaluations suggests that participants recognize the complementary nature of regulatory and ethical approaches to responsible AI.

RQ.3 Summary: Participants consistently perceived strong alignment between LGPD principles and AI ethical principles. Most respondents selected high agreement levels (4 or 5), indicating that data protection concepts such as purpose limitation, adequacy, necessity, transparency, security, prevention, non-discrimination, and accountability are viewed as directly compatible with core AI ethics values. The strongest alignment was observed in the pair *Security (LGPD)* and *Privacy and Data Governance (AI ethics)*, where nearly four out of five participants rated the correspondence as high or very high. Results suggest that participants understand LGPD as a solid foundation for ethical AI governance.

5.3 RQ4. How do participants evaluate the sufficiency of LGPD principles for guiding ethical AI, what ethical gaps do they identify, and how do they expect the law to evolve in response to AI-related challenges?

To address RQ4, Study 2 included four groups of questions assessing: (a) whether LGPD principles are perceived as sufficient for guiding ethical AI development (Q19), (b) whether AI ethical principles complement and extend LGPD (Q20), (c) which LGPD principles participants consider most relevant for ethical AI (Q21), and (d) which AI ethical principles participants believe are not covered by the LGPD (Q22). We also asked whether AI ethics should inform future revisions of the LGPD (Q23).

Perceived sufficiency of LGPD principles (Q19). Responses were widely distributed, indicating no consensus on whether LGPD alone is enough to guide ethical AI, as shown in Figure 5. Only 41% selected 4 or 5 (agree/strongly agree), while 59% selected 1–3. The distribution was: 1 (13%), 2 (28%), 3 (18%), 4 (26%), and 5 (15%). These results suggest that although LGPD provides an important regulatory foundation, participants recognize limitations when it comes to addressing broader ethical challenges of AI systems.

AI ethical principles as extensions to LGPD (Q20). Participants strongly agreed that AI ethics complements the LGPD, with 79% selecting 4 or 5 (Figure 5). Only 9% disagreed (1 or 2). This indicates that participants view AI ethics frameworks as necessary additions to legal compliance, particularly for principles related to fairness, robustness, and societal impact.

Most relevant LGPD principles for ethical AI (Q21). Participants identified *Security* (63%), *Transparency* (48%), and *Data Quality* (44%) as the most critical LGPD principles for ethical AI development (Figure 6). Other principles such as *Non-discrimination* (35%) and *Accountability* (36%) were also frequently selected. These priorities reflect a strong emphasis on technical safeguards and governance structures components that participants perceive as important for trustworthy AI.

AI ethical principles not covered by LGPD (Q22). Respondents identified several ethical principles they believe remain insufficiently addressed by the LGPD, as shown in Figure 7. The most frequently selected were *Non-maleficence* (28%), *Inclusion and Diversity* (26%), and *Solidarity* (26%), followed by *Autonomy* (23%), *Justice and Equity* (21%), and *Prosperity* (20%). Many of these belong to the socio-ethical dimension of AI highlighting the gap between legal protection frameworks and broader human-centered ethical principles.

Should AI ethics inform future revisions of LGPD? (Q23). Most participants (71%) answered "Yes," while 25% responded "Maybe" and only 4% answered "No", as shown in Figure 8. These findings reinforce the perception that LGPD, although foundational, may need future updates to address emerging risks and ethical considerations introduced by AI technologies.

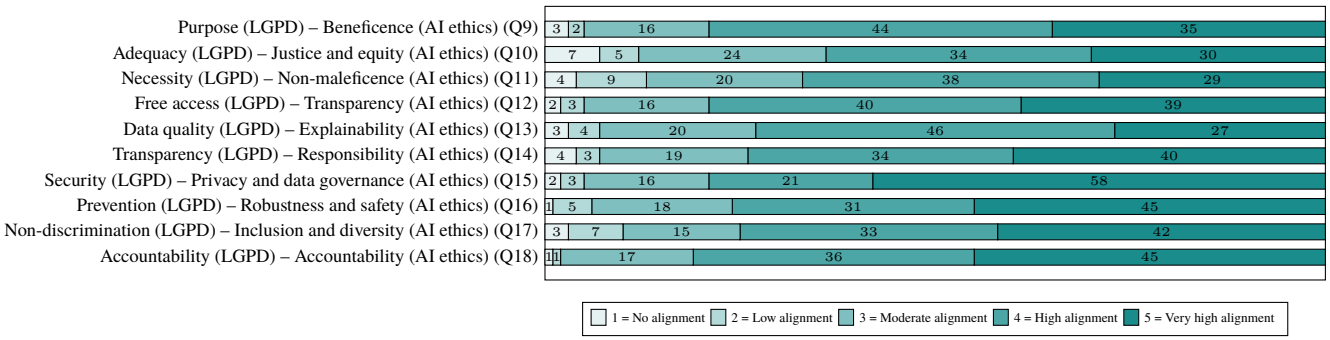

Figure 4. Perceived alignment between LGPD principles and AI ethical principles (Q9–Q18).

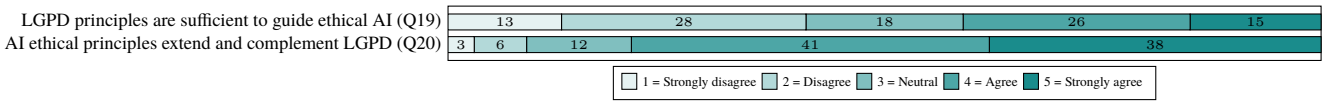

Figure 5. Perceptions of the sufficiency of LGPD principles and the complementary role of AI ethics (Q19–Q20).

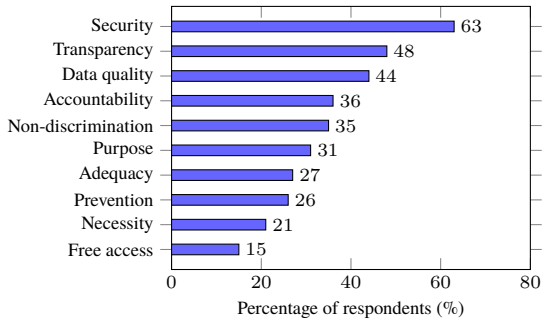

Figure 6. LGPD principles considered most relevant for ethical AI development (Q21, $n = 100$).

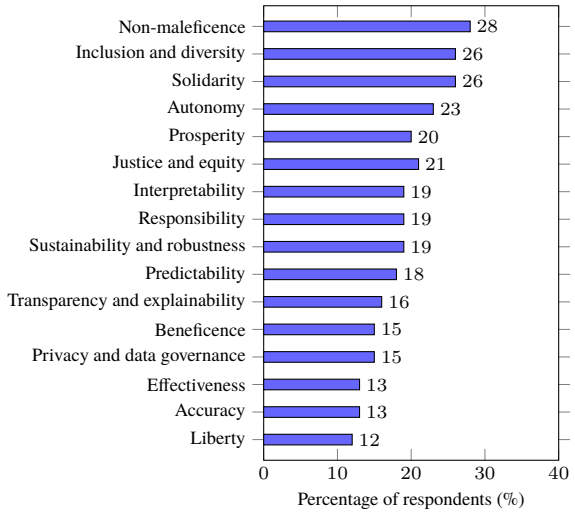

Figure 7. AI ethical principles perceived as not fully covered by LGPD (Q22, $n = 100$).

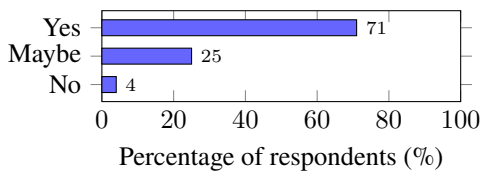

Figure 8. Perceptions on whether AI ethical principles should inform future LGPD revisions (Q23, $n = 100$).

Participants' open-ended responses to Q24 reveal a clear pattern: although the LGPD is widely recognized as a strong foundation for personal data protection, most respondents believe it is not yet fully equipped to address the ethical and sociotechnical challenges introduced by Artificial Intelligence. The thematic analysis resulted in four major categories, as shown in Table 5, which together reflect broad consensus on the need for regulatory evolution, whether through updates to the LGPD itself or through complementary governance mechanisms.

The dominant category, *Need to update the LGPD due to AI-related ethical challenges*, aggregates the majority of responses. Participants argue that the LGPD was created in a technological context prior to the emergence of modern AI techniques such as large-scale machine learning, generative models, and autonomous decision-making systems. As a result, the law does not yet offer explicit guidance on issues such as algorithmic transparency, fairness, automated profiling, model accountability, and the use of personal data for training AI models. Several respondents stressed that only targeted updates in the law will ensure the protection of fundamental rights in the face of increasingly opaque and high-impact AI systems. As R#38 participant stated:

> *"Yes, I believe the LGPD needs to be updated to keep pace with advances in Artificial Intelligence. Today, AI influences important decisions, and we often do not even know how these systems operate or handle our data. The current law protects privacy well, but it still fails to address issues such as algorithmic bias, transparency in automated decisions, and corporate responsibility. Updating the LGPD would ensure that technological progress does not overlook fundamental rights and ethical principles."*

A second category reflects the view that instead of modifying the LGPD itself, Brazil should develop a *complementary regulatory ecosystem*, including sector specific guidelines, governance frameworks, and a dedicated AI legal framework (e.g., PL 2338/2023)[1]. These respondents note that opening and revising the LGPD could create legislative instability or yield overly rigid rules that might become obsolete quickly given the fast pace of AI evolution. R#12 participant summarized this position as follows:

[1] https://www25.senado.leg.br/web/atividade/materias/-/materia/157233

"Instead of changing the LGPD now, which is slow and politically complex, it is more strategic to complement it with governance guidelines or a specific AI framework. The LGPD should remain the central reference, but AI needs additional rules for monitoring, auditing, and risk mitigation."

A smaller subset of respondents argued that the LGPD is already sufficient and that AI systems must adapt to the law, not the other way around. For these participants, the LGPD's technological neutrality and principle based structure already encompass the major risks associated with data driven AI systems. Finally, a minority expressed uncertainty or skepticism regarding the need for legal updates, whether due to limited knowledge of the topic or concerns about the government's ability to regulate AI effectively.

These findings indicate that while participants support the governance of AI, they differ on *how* this should occur through modifications to the LGPD or through complementary regulatory instruments. Nevertheless, there is strong agreement that AI introduces new ethical, social, and legal risks that require more explicit mechanisms related to transparency, explainability, fairness, and accountability.

RQ.4 Summary: Participants perceive the LGPD as an important but insufficient foundation for guiding ethical practices in AI. They believe AI ethics introduces additional concerns such as fairness, transparency, explainability, accountability, and human-centered values that are not fully addressed by existing data protection principles. Respondents emphasized the need for stronger governance mechanisms and clearer guidance for managing algorithmic risks. While some argue for updating the LGPD, others prefer complementary AI specific regulation to avoid legislative rigidity. The findings reveal broad expectations for more explicit, adaptive, and ethically aligned regulation to accompany the evolution of AI systems.

6 Comparative Analysis: Study 1 vs. Study 2

This section compares the main findings of Study 1 and Study 2, highlighting how the two surveys complement each other in terms of sample profile, perceived alignment between LGPD principles and AI ethics, and perceived sufficiency and gaps in the current regulatory framework. Together, the studies provide a richer picture of how computing students and practitioners interpret the relationship between data protection law and ethical principles for AI.

Before discussing the comparative findings, it is important to emphasize that the alignment identified between LGPD principles and AI ethical principles in this study reflects participants' conceptual perceptions rather than empirical evidence of operational integration or enforceability in real-world systems. While perceptions influence professional attitudes and may shape future governance trajectories, they do not necessarily indicate that such alignment is systematically implemented within software development practices or regulatory oversight mechanisms. Therefore, the findings should be interpreted as exploratory evidence of interpretative convergence within the computing community, rather than as proof of effective regulatory harmonization.

6.1 Samples and Knowledge Profiles

Study 1 was conducted with a small, predominantly student sample ($n = 30$), mainly from Computer Science and related undergraduate programs. As reported in Section 4, participants showed limited prior knowledge of both LGPD and AI ethical principles, with a sizable proportion declaring they did not know these concepts or knew them only "a little". This first survey therefore reflects perceptions from individuals at an early stage of their professional trajectory, still consolidating their understanding of data protection and ethics in AI.

Study 2 expanded the scope and scale of the investigation, reaching $n = 100$ respondents with a more heterogeneous profile, including both students and professionals occupying a variety of software project roles (e.g., developers, analysts, project managers, data scientists), as summarized in Table 4. Knowledge levels about LGPD and AI ethics were markedly higher in this second sample: most respondents reported knowing LGPD principles, and almost half indicated familiarity with AI ethical principles. This contrast suggests that Study 2 captures perceptions from a more mature audience in terms of exposure to privacy regulation and AI debates.

The two samples allow a triangulated view: Study 1 foregrounds how LGPD and AI ethics are perceived by those entering the field, whereas Study 2 reveals how these principles are interpreted by individuals already embedded in software development practice.

6.2 Perceived Alignment Between LGPD Principles and AI Ethics

Across both studies, respondents consistently perceived a strong conceptual alignment between LGPD principles and ethical principles for AI. In Study 1, participants spontaneously associated LGPD with core ethical dimensions such as privacy, transparency, data minimization, security, and accountability (Section 4). Open-ended comments emphasized, for instance, the need for transparency in both corporate data practices and AI systems, the importance of minimizing data collection, and the expectation that developers should be accountable for AI-driven decisions.

Study 2 extended this initial insight through a more fine-grained, principle-to-principle mapping (Q9–Q18), systematically pairing each LGPD principle with a corresponding AI ethical principle. The results showed consistently high agreement levels across all ten pairs, with most respondents rating the alignment as high or very high (Section 5). Particularly strong correspondence was observed for pairs involving security and data governance, prevention and robustness, and non-discrimination and inclusion/diversity.

While Study 1 provided an exploratory indication that participants intuitively connect LGPD and AI ethics at a high level, Study 2 confirmed and quantified this perception with structured Likert items. Both studies converge on the idea that LGPD is not perceived merely as a compliance instru-

Category	#	Examples of Terms
1. LGPD should be updated to address AI-specific ethical challenges	62	"new risks not covered", "AI evolves faster than the law", "training data and automated decisions require clearer rules", "lack of transparency and explainability", "bias and discrimination risks", "need to strengthen accountability", "periodic updates are necessary"
2. Complementing the LGPD with targeted AI regulation or governance frameworks	21	"LGPD as a foundation but insufficient alone", "AI Legal Framework (Marco Legal da IA)", "sectoral guidelines and best practices", "flexible non-legislative instruments", "avoid rigid law changes that may become obsolete"
3. LGPD is already sufficient; AI should adapt to the existing law	9	"LGPD is technologically neutral", "the problem is enforcement, not legislation", "AI must comply with the LGPD, not the opposite", "current issues already violate existing norms"
4. Skepticism, uncertainty, or criticism of regulatory capacity	8	"risk of poorly informed regulation", "bureaucrats do not understand technology", "prefer not to take a position", "uncertainty about how AI should be regulated", "fear of ineffective or overly rigid laws"

Table 5. Qualitative categories derived from participants' explanations on whether the LGPD should be updated to address AI ethical challenges (Q24).

ment, but also as a meaningful reference for ethical expectations in AI development.

6.3 Challenges, Gaps, and the Role of LGPD in Ethical AI Governance

The two studies also align in revealing that, despite strong perceived overlap, LGPD is not seen as sufficient on its own to address all ethical and sociotechnical challenges of AI.

In Study 1, participants pointed to concrete difficulties in operationalizing LGPD principles in AI contexts, particularly around explicit consent, data security, accountability, and algorithmic explainability. Respondents highlighted the tension between continuous learning processes in AI and the need to obtain, track, and update consent; they also questioned how responsibility should be assigned when autonomous systems cause harm, and expressed concern about the opacity of AI models.

Study 2 deepened this discussion in two ways. First, the quantitative questions on the sufficiency of LGPD and the complementary role of AI ethics (Q19–Q20) showed that respondents do not converge on the view that LGPD principles alone are enough to guide ethical AI, while strongly agreeing that AI ethical frameworks extend and complement the law. Second, the questions on LGPD principles most relevant for ethical AI (Q21) and AI ethical principles not fully covered by LGPD (Q22) revealed an asymmetry between *technical* and *socio-ethical* dimensions: participants emphasized security, transparency, and data quality on the LGPD side, whereas the main perceived gaps involved non-maleficence, inclusion and diversity, solidarity, autonomy, and justice and equity.

The qualitative analysis of Q24 further clarified how respondents envision the evolution of regulation. The dominant view is that LGPD needs to be updated or complemented to explicitly address AI-specific risks such as algorithmic bias, opacity in automated decisions, profile based inference, and the use of personal data in model training. At the same time, a significant subset of participants advocates for a complementary regulatory ecosystem (e.g., specific AI frameworks, sectoral guidelines, governance mechanisms) rather than frequent amendments to LGPD itself. A smaller group considers the current law sufficient in principle, arguing that the main problem lies in enforcement and compliance rather than in the legal text.

6.4 Synthesis of Cross-Study Insights

Combining the findings of Study 1 and Study 2 yields three main cross-cutting insights. First, across different profiles and knowledge levels, participants converge in viewing LGPD as a meaningful foundation for ethical AI governance, especially regarding privacy, transparency, security, and data minimization. Second, as participants' experience and familiarity with the topic increase, they tend to articulate more clearly that LGPD, while necessary, does not fully capture the socio-ethical and human centered dimensions emphasized in AI ethics frameworks, such as fairness, inclusion, solidarity, and autonomy. Third, both studies indicate a strong expectation that future governance of AI in Brazil should integrate legal protections (LGPD) with explicit ethical principles and dedicated mechanisms for transparency, explainability, and accountability in algorithmic decision-making.

The comparative analysis suggests that LGPD is perceived not as an endpoint, but as a starting point for building a broader, principle based and risk sensitive ecosystem for responsible AI in the Brazilian context.

From a software engineering perspective, the findings suggest that regulatory frameworks such as the LGPD, while conceptually aligned with several AI ethical principles, require explicit translation into development practices, requirements elicitation processes, and governance mechanisms. The perceived alignment identified in this study does not automatically guarantee operational integration within software projects. Therefore, structured approaches such as ethics-by-design, requirements engineering guidelines, traceability mechanisms, and compliance-aware development processes may be necessary to bridge the gap between normative principles and implementation practices.

From an educational standpoint, the results reinforce the importance of integrating discussions on data protection regulation and AI ethics within computing curricula. As students and early-career professionals demonstrate awareness of conceptual alignment but uncertainty regarding regulatory sufficiency, educational programs should emphasize not only

ethical principles but also their translation into concrete software engineering practices and regulatory contexts.

7 Limitations and Threats to Validity

Following Wohlin's recommendations for empirical studies (Wohlin *et al.*, 2012), we analyzed the threats to validity across four dimensions: conclusion, internal, construct, and external validity. Because this research is based on two complementary surveys (Study 1 and Study 2), the threats and corresponding mitigation strategies reflect the methodological evolution between both phases. **Conclusion Validity**: A primary threat concerns the differing sample sizes across the two studies. Study 1 relied on a small sample ($n = 30$), which limits the statistical stability and generalizability of descriptive findings. However, Study 1 was intentionally designed as an exploratory phase aimed at identifying preliminary perception patterns and informing the redesign and expansion implemented in Study 2. Study 2 expanded to $n = 100$, enabling more robust interpretations but still depending primarily on descriptive statistics. Furthermore, both studies rely on self-reported data, which may introduce noise and random variation in responses. To mitigate these risks, Study 2 was designed explicitly to strengthen statistical reliability by expanding the sample, diversifying participant profiles, and replicating key constructs of Study 1. Patterns observed consistently across both studies increase confidence in the stability of findings. Additionally, Likert scale distributions were analyzed in full (rather than collapsed categories), reducing data loss and supporting more grounded conclusions.

Internal Validity: Selection bias is an inherent risk: Study 1 sampled only undergraduate computing students, while Study 2 although more diverse still primarily includes individuals linked to Computing. Self-selection bias may also occur, as participants who care more about privacy or AI ethics may be more inclined to respond. In Study 2, recruitment was conducted primarily through social networks and professional contacts, which may further intensify self-selection effects. Individuals more engaged with discussions on AI, privacy, or governance may have been more likely to encounter and respond to the survey. This recruitment strategy may therefore overrepresent participants with prior interest or awareness in ethical and regulatory issues, potentially influencing alignment and sufficiency perceptions. To partially mitigate this risk, we disseminated the survey across diverse professional groups and networks, aiming to reach participants with heterogeneous roles, experience levels, and organizational backgrounds.

Another potential threat concerns respondent fatigue, given the number of Likert items in Study 2 (especially Q9–Q18), which may influence response consistency. Study 2 purposely broadened recruitment to professionals from different roles (developers, analysts, managers, data scientists), reducing the student only bias of Study 1. The informed consent form emphasized anonymity and the absence of evaluative consequences, reducing social desirability bias. The questionnaire was piloted and optimized to avoid redundancy and excessive length. No incentives were offered, avoiding coercion and reducing systematic bias.

Construct Validity risks arise from participants' heterogeneous levels of familiarity with LGPD and AI ethics, especially in Study 1, where many reported low prior knowledge. Misinterpretation of constructs (e.g., explainability, non-maleficence, necessity) may also occur. Another threat concerns mono-method bias, since both studies rely exclusively on survey instruments rather than triangulating measurement through interviews or observational data. To address these threats, Study 2 incorporated clearer operational definitions and phrasing, particularly in the paired items (Q9–Q18), explicitly connecting LGPD principles to their corresponding AI ethical concepts. The questionnaire was refined through expert review to ensure conceptual clarity. Moreover, open-ended questions (Q24) provided qualitative depth, enabling triangulation of constructs by capturing participants' interpretations in their own words. This reduced the risk of construct ambiguity and enhanced the semantic validity of the findings.

External Validity: The generalizability of the results remains limited. While Study 2 expanded significantly beyond Study 1, the sample still reflects a population predominantly from Brazil and concentrated in Computing related fields. Therefore, the findings may not generalize to professionals from non-technical domains, to other countries, or to organizational settings with different regulatory cultures. Study 2 broadened demographic categories, age ranges, professional roles, and experience levels, mitigating the narrow scope of Study 1. By comparing two independent samples (students vs. mixed students and practitioners), the study partially reduces context-specific effects. The research design focuses on conceptual perceptions (alignment, sufficiency, gaps), which are more stable across contexts than behavior-based measures, increasing transferability. Nevertheless, we acknowledge that future studies including cross-country comparisons, interviews, or organizational case studies are important to strengthen external validity.

8 Conclusion and Future Work

This research provided a two-phase empirical investigation into how students and professionals in Computing perceive the relationship between LGPD principles and AI ethical principles, examining areas of alignment, practical challenges, perceived gaps, and expectations for regulatory evolution in the context of Artificial Intelligence. The combined results of Study 1 and Study 2 reveal a clear pattern: although participants consistently recognize strong conceptual alignment between LGPD and AI ethics, particularly regarding privacy, transparency, security, prevention, non-discrimination, and accountability. This alignment does not fully translate into perceived sufficiency for guiding ethical AI in practice.

Across both studies, participants agreed that LGPD offers a solid foundational framework for data protection and can serve as an anchor for responsible AI governance. However, Study 2 shows that most respondents believe the LGPD alone is not enough to address the socio-ethical, technical, and organizational risks introduced by modern AI systems, especially those involving automated decision-making,

model opacity, and large scale data processing. Key gaps identified include issues related to explainability, algorithmic fairness, bias mitigation, broader human-centered values (e.g., autonomy, inclusion, solidarity), and governance structures capable of ensuring accountability throughout the AI lifecycle.

Both studies highlighted practical challenges: ensuring meaningful and dynamic consent in systems that continually evolve, safeguarding increasingly large and sensitive datasets, defining responsibility for autonomous or semi-autonomous decisions, and enabling auditing and oversight of opaque AI models. The qualitative analysis of Study 2 reinforces these concerns, revealing strong expectations for regulatory evolution either through targeted updates to the LGPD or through complementary AI-specific frameworks such as the proposed Brazilian AI Legal Framework (PL 2338/2023). Participants expressed a desire for more explicit guidelines on transparency, algorithmic auditing, bias detection, model documentation, and human oversight.

The findings emphasize that the intersection between data protection and AI ethics requires not only legal and governance mechanisms but also technical solutions such as explainable AI (XAI), robust cybersecurity practices, and tools that support continuous monitoring of algorithmic behavior. Moreover, the results suggest the need for interdisciplinary collaboration among legal practitioners, software engineers, data scientists, and policy makers to operationalize ethical principles in real-world AI use cases.

Building on these findings, several avenues for future research emerge. First, expanding the sample to include legal experts, regulatory authorities, public sector managers, and professionals from non-technical fields would broaden external validity and enrich the understanding of how AI governance needs differ across sectors. Second, in-depth qualitative methods such as interviews, case studies, or ethnographic approaches should be employed to explore how organizations implement (or struggle to implement) LGPD and AI ethics principles in practice. Third, empirical evaluations of real-world AI systems could provide evidence on the effectiveness of technical mechanisms for explainability, fairness auditing, and consent management. Finally, future work may focus on developing or validating governance frameworks, toolkits, and maturity models that support the integration of data protection principles with human-centered AI ethics, thereby contributing to a more comprehensive and actionable approach to responsible AI in Brazil.

Overall, this research offers empirical insight into how LGPD and AI ethics intersect from the perspective of those who develop, deploy, and study digital systems. The results reinforce the need for adaptive, transparent, and multi-layered regulatory and technical mechanisms to ensure that AI technologies evolve in a manner that is aligned with both legal obligations and societal expectations.

Declarations

Acknowledgements

This study was financed in part by the Conselho Nacional de Desenvolvimento Científico e Tecnológico CNPq (Grant Nº 300883/2025-0).

Authors' Contributions

Ana Caroline contributed to the conceptualization, methodology, data collection, writing the original draft and editing of the manuscript preparation of this study. João Rossi and Edna Dias contributed to the methodology, formal analysis, supervision, validation, writing review and editing of the manuscript. All authors participated in the discussion of results, provided feedback to improve the paper and approved the final version of the manuscript.

Competing interests

The authors declare that they have no competing interests.

Availability of data and materials

The data that support the findings of this study are openly available in Zenodo (DOI: https://doi.org/10.5281/zenodo.17847734).

Further relevant information

The authors acknowledge the use of generative AI tools for grammar refinement and language improvement during the preparation of this manuscript. The use of these tools was strictly supervised, and all content was reviewed and validated by the authors.

References

Beppu, F. R., Maciel, C., and Viterbo, J. (2021). Contributions of the brazilian act for the protection of personal data for treating digital legacy. *Journal on Interactive Systems*, 12(1):112–124. DOI: https://doi.org/10.5753/jis.2021.1654.

Braz, A. and Canedo, E. (2025). Mapping lgpd principles to ethical principles in the context of artificial intelligence. In *Anais do VI Workshop sobre as Implicações da Computação na Sociedade*, pages 1–13, Porto Alegre, RS, Brasil. SBC. DOI: https://doi.org/10.5753/wics.2025.7160.

Brey, P. and Dainow, B. (2023). Ethics by design for artificial intelligence. *AI and Ethics*, pages 1–13. DOI: https://doi.org/10.1007/s43681-023-00330-4.

Brown, N., Xie, B., Sarder, E., Fiesler, C., and Wiese, E. S. (2024). Teaching ethics in computing: A systematic literature review of ACM computer science education publications. *ACM Trans. Comput. Educ.*, 24(1):6:1–6:36. DOI: https://doi.org/10.1145/3634685.

Cappelli, M. A. and Serugendo, G. D. M. (2025). A semi-automated software model to support AI ethics compliance assessment of an AI system guided by ethical principles of AI. *AI Ethics*, 5(2):1357–1380. DOI: https://doi.org/10.1007/S43681-024-00480-Z.

Carrasco, L. B. (2025). Towards responsible AI: A conceptual framework for mitigating ethical risks in generative artificial intelligence systems. In *31st Americas Conference on Information Systems: Intelligent Technologies for a Better Future, AMCIS 2025, Montreal, QC, Canada, August 14-16, 2025*. Association for Information Systems. DOI: https://aisel.aisnet.org/amcis2025/ict_global/ict_global/8.

Carvalho, L. P., Oliveira, J., Santoro, F. M., and Cappelli, C. (2021). Social network analysis, ethics and lgpd, considerations in research. *iSys-Brazilian Journal of Information Systems*, 14(2):28–52. DOI: https://doi.org/10.5753/isys.2021.1235.

Carvalho, L. P., Rodrigues, K. R. d. H., Oliveira, J.,

and Santoro, F. M. (2025). Enhancing ethical communication in brazilian computing research: A framework for human involvement reporting. *Journal on Interactive Systems*, 16(1):749–772. DOI: https://doi.org/10.5753/jis.2025.5977.

Danilevskyi, M., Pérez-Téllez, F., and Buscaldi, D. (2025). Implementing ethical principles in AI: an initial discussion. *AI Ethics*, 5(4):3549–3555. DOI: https://doi.org/10.1007/S43681-025-00710-Y.

de Araújo Neto, R. J. and Barbosa Aguiar, J. J. (2024). Os impactos da lei geral de proteção de dados (lgpd) na segurança da informação: uma revisão da literatura. *GeSec: Revista de Gestao e Secretariado*, 15(2). DOI: https://doi.org/10.7769/gesec.v15i2.3442.

de Cerqueira, J. A. S., Azevedo, A. P. D., Leão, H. A. T., and Canedo, E. D. (2022). Guide for artificial intelligence ethical requirements elicitation - RE4AI ethical guide. In *55th Hawaii International Conference on System Sciences, HICSS 2022, Virtual Event / Maui, Hawaii, USA, January 4-7, 2022*, pages 1–10. ScholarSpace. DOI: http://hdl.handle.net/10125/80015.

de Cerqueira, J. A. S., Leão, H. A. T., and Canedo, E. D. (2021). Ethical guidelines and principles in the context of artificial intelligence. In *SBSI 2021: XVII Brazilian Symposium on Information Systems, Uberlândia, Brazil, June 7 - 10, 2021*, pages 36:1–36:8. ACM. DOI: https://doi.org/10.1145/3466933.3466969.

de Oliveira, K. A. C. (2024). Formação de jurisprudência administrativa pela anpd: estudo de casos das sanções aplicadas. *Revista Digital de Direito Administrativo*, 11(2):89–109. DOI: https://doi.org/10.11606/issn.2319-0558.v11i2p89-109.

Díaz-Rodríguez, N., Del Ser, J., Coeckelbergh, M., López de Prado, M., Herrera-Viedma, E., and Herrera, F. (2023). Connecting the dots in trustworthy artificial intelligence: From ai principles, ethics, and key requirements to responsible ai systems and regulation. *Information Fusion*, 99:101896. DOI: https://doi.org/10.1016/j.inffus.2023.101896.

Falcão, F. D. S. and Canedo, E. D. (2024). Investigating software development teams members' perceptions of data privacy in the use of large language models (llms). In *Proceedings of the XXIII Brazilian Symposium on Software Quality, SBQS 2024, Salvador, Bahia, Brazil, November 5-8, 2024*, pages 373–382. ACM. DOI: https://doi.org/10.1145/3701625.3701675.

Federal, G. (2021). Guia de boas práticas para implementação na administração pública federal. 2020. Available in `https://www.gov.br/secom/pt-br/central-de-conteudo/redes/guia` Accessed on 15 December 2025.

Fernandes, A. C. and MEIRA, T. M. (2023). Impactos da inteligência artificial na advocacia brasileira: desafios e oportunidades. *Revista Jurídica do Nordeste Mineiro*, 7(1). DOI: https://doi.org/10.61164/rjnm.v7i1.2010.

Finocchiaro, G. (2024). The regulation of artificial intelligence. *Ai & Society*, 39(4):1961–1968. DOI: https://doi.org/10.1007/s00146-023-01650-z.

Floridi, L., Cowls, J., King, T. C., and Taddeo, M. (2021). How to design ai for social good: Seven essential factors. *Ethics, Governance, and Policies in Artificial Intelligence*, pages 125–151. DOI: https://doi.org/10.1007/s11948-020-00213-5.

Gonçalves, C. D., Menescal, E. d. P., de Mendonça, F. L. L., and Canedo, E. D. (2024). Trust in ai: Perspectives of c-level executives in brazilian organizations. In *Proceedings of the XXIII Brazilian Symposium on Software Quality*, SBQS '24, page 147–157, New York, NY, USA. Association for Computing Machinery. DOI: https://doi.org/10.1145/3701625.3701654.

González, A. L., Moreno, M., Román, A. C. M., Fernández, Y. H., and Pérez, N. C. (2024). Ethics in artificial intelligence: an approach to cybersecurity. *Inteligencia Artificial*, 27(73):38–54. DOI: https://doi.org/10.4114/intartif.vol27iss73pp38-54.

Guimarães, G., Filho, G. R., Marques, G., and Canedo, E. (2025). May i speak? perceptions on ethical concerns and power while developing software in ai teams. In *Anais do XXIV Simpósio Brasileiro de Qualidade de Software*, pages 44–54, Porto Alegre, RS, Brasil. SBC. DOI: https://doi.org/10.5753/sbqs.2025.13576.

Jobin, A., Ienca, M., and Vayena, E. (2019). The global landscape of ai ethics guidelines. *Nature machine intelligence*, 1(9):389–399. DOI: https://doi.org/10.1038/s42256-019-0088-2.

Karimov, A., Saarela, M., Aliyev, S., and Baker, R. (2025). Ethical considerations and student perceptions of engagement data in learning analytics. In *Proceedings of the Annual Hawaii International Conference on System Sciences*. University of Hawai i at Mānoa. DOI: https://hdl.handle.net/10125/109419.

Khan, A. A., Akbar, M. A., Fahmideh, M., Liang, P., Waseem, M., Ahmad, A., Niazi, M., and Abrahamsson, P. (2023). Ai ethics: an empirical study on the views of practitioners and lawmakers. *IEEE Transactions on Computational Social Systems*, 10(6):2971–2984. DOI: https://doi.org/10.1109/TCSS.2023.3251729.

Khan, A. A., Badshah, S., Liang, P., Waseem, M., Khan, B., Ahmad, A., Fahmideh, M., Niazi, M., and Akbar, M. A. (2022). Ethics of AI: A systematic literature review of principles and challenges. In *EASE 2022: The International Conference on Evaluation and Assessment in Software Engineering 2022, Gothenburg, Sweden, June 13 - 15, 2022*, pages 383–392. ACM. DOI: https://doi.org/10.1145/3530019.3531329.

Kipman, F., Marques, G., and Canedo, E. (2025). Computing students' perceptions of ethical principles in ai and curricular coverage. In *Anais do XXIV Simpósio Brasileiro de Qualidade de Software*, pages 431–441, Porto Alegre, RS, Brasil. SBC. DOI: https://doi.org/10.5753/sbqs.2025.13611.

Kitchenham, B. and Charters, S. (2007). Guidelines for performing systematic literature reviews in software engineering. *EBSE Technical Report EBSE-2007-01*.

Macedo, P. N. (2018). Brazilian general data protection law (lgpd). *National Congress, Accessed on 15 December 2025*.

Machado, H., Silva, S., and Neiva, L. (2025). Publics'

views on ethical challenges of artificial intelligence: a scoping review. *AI Ethics*, 5(1):139–167. DOI: https://doi.org/10.1007/S43681-023-00387-1.

Martins, M. E., Aguiar, Y. P. C., and Saraiva, J. (2025). Assessment of competences for LGPD DPO through ANPD standard and information systems curriculum. In *Proceedings of the 21st Brazilian Symposium on Information Systems, SBSI 2025, Recife, Brazil, May 19-23, 2025*, pages 565–574. SBC. DOI: https://doi.org/10.5753/SBSI.2025.246585.

Maturo, F., Porreca, A., and Porreca, A. (2025). The risks of artificial intelligence in research: ethical and methodological challenges in the peer review process. *AI Ethics*, 5(5):5389–5396. DOI: https://doi.org/10.1007/S43681-025-00775-9.

McGrath, Q. P., Hevner, A. R., and de Vreede, G. (2025). Designing an enhanced enterprise risk management system to mitigate ethical risks of artificial intelligence applications. *IEEE Trans. Engineering Management*, 72:1813–1830. DOI: https://doi.org/10.1109/TEM.2025.3565221.

Nascimento, S. M., de Paiva, T. M. G., Kasuga, M. P. M., Silva, T. d. A. F., Crozara, C. M. G., Byk, J., and da Conceição Furtado, S. (2024). Inteligência artificial e suas implicações éticas e legais: revisão integrativa. *Revista Bioética*, 32. DOI: https://doi.org/10.1590/1983-803420243729ES.

Neves, B. C. (2023). Mapeamento sistemático da literatura sobre a inteligência artificial na medicina clinica: papel e princípios éticos dos algoritmos. *Revista Fontes Documentais*, 6(Ed. Especial):78–79.

Nguyen, A., Ngo, H. N., Hong, Y., Dang, B., and Nguyen, B.-P. T. (2023). Ethical principles for artificial intelligence in education. *Education and information technologies*, 28(4):4221–4241. DOI: https://doi.org/10.1007/s10639-022-11316-w.

Pant, A., Hoda, R., Tantithamthavorn, C., and Turhan, B. (2025). Navigating fairness: practitioners' understanding, challenges, and strategies in AI/ML development. *Empir. Softw. Eng.*, 30(3):102. DOI: https://doi.org/10.1007/s10664-025-10650-0.

Petersen, K., Feldt, R., Mujtaba, S., and Mattsson, M. (2008). Systematic mapping studies in software engineering. In *12th International Conference on Evaluation and Assessment in Software Engineering, EASE 2008, University of Bari, Italy, 26-27 June 2008*, Workshops in Computing. BCS.

Porto, D., Prado, R., Marques, G., Serrano, A., Mendonça, F., and Canedo, E. (2025). Ethical requirements in the age of artificial intelligence: A systematic literature review. In *Anais do XXI Simpósio Brasileiro de Sistemas de Informação*, pages 663–672, Porto Alegre, RS, Brasil. SBC. DOI: https://doi.org/10.5753/sbsi.2025.246613.

Quintino, M. E. G., Garcia, A. G. P. V., Primola, A. M. S. P., Chaves, E. C., Souza, N. M., Oliveira, L. L. G., and Sousa, C. V. (2024). Implicações éticas do uso da inteligência artificial (ia) em textos científicos: uma revisão integrativa de literatura. In *Abec Meeting*. DOI: https://doi.org/10.21452/abecmeeting2024.258.

Rapôso, C. F. L., de Lima, H. M., de Oliveira Junior, W. F., Silva, P. A. F., and de Souza Barros, E. E. (2019). Lgpd-lei geral de proteção de dados pessoais em tecnologia da informação: Revisão sistemática. *RACE-Revista de Administração do Cesmac*, 4:58–67. DOI: https://doi.org/10.3131/race.v4i0.1035.

Rocha, L. D., Silva, G. R. S., and Canedo, E. D. (2023). Privacy compliance in software development: A guide to implementing the LGPD principles. In *Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing, SAC 2023, Tallinn, Estonia, March 27-31, 2023*, pages 1352–1361. ACM. DOI: https://doi.org/10.1145/3555776.3577615.

Russell, S., Norvig, P., and Intelligence, A. (1995). A modern approach. *Artificial Intelligence. Prentice-Hall, Egnlewood Cliffs*, 25(27):79–80.

Ryan, M. and Stahl, B. C. (2021). Artificial intelligence ethics guidelines for developers and users: clarifying their content and normative implications. *J. Inf. Commun. Ethics Soc.*, 19(1):61–86. DOI: https://doi.org/10.1108/JICES-12-2019-0138.

Sarlet, G. B. S. and Ruaro, R. L. (2021). A proteção de dados sensíveis no sistema normativo brasileiro sob o enfoque da lei geral de proteção de dados (lgpd)–l. 13.709/2018. *Revista Direitos Fundamentais & Democracia*, 26(2):81–106. DOI: https://doi.org/10.25192/issn.1982-0496.rdfd.v26i22172.

Spósito, S. L., Moreira, F. R., and Canedo, E. D. (2025). Designing a training journey for privacy and information security practitioners in the federal public administration. In *Proceedings of the 21st Brazilian Symposium on Information Systems, SBSI 2025, Recife, Brazil, May 19-23, 2025*, pages 95–104. SBC. DOI: https://doi.org/10.5753/SBSI.2025.246040.

Stavrakakis, I., Gordon, D., Tierney, B., Becevel, A., Murphy, E., Dodig-Crnkovic, G., Dobrin, R., Schiaffonati, V., Pereira, C., Tikhonenko, S., *et al.* (2022). The teaching of computer ethics on computer science and related degree programmes. a european survey. *International Journal of Ethics Education*, 7(1):101–129. DOI: https://doi.org/10.1007/s40889-021-00135-1.

UNESCO (2022). Recomendação sobre a Ética da inteligência artificial. Available in `https://unesdoc.unesco.org/ark:/48223/pf0000381137_por` Accessed on 10 January 2025.

Wohlin, C., Runeson, P., Höst, M., Ohlsson, M. C., Regnell, B., and Wesslén, A. (2012). *Experimentation in Software Engineering*. Springer.