Mapping LGPD Principles to Ethical Principles in the Context of Artificial Intelligence

Ana Caroline da Rocha Braz, , Edna Dias Canedo

[1]University of Brasília (UnB), Department of Computer Science, Brasília, DF, Brazil
E-mail: ana.caroline.6@hotmail.com, ednacanedo@unb.br

Abstract. *The intersection between the ethical principles of the Brazilian General Data Protection Law (LGPD) and Artificial Intelligence (AI) presents a significant challenge in regulating data usage and addressing ethical risks. This study investigates the compatibility between these principles by identifying their points of convergence and divergence, as well as the practical challenges involved in their application. The research draws on a combination of literature review, document analysis, and a survey exploring participants' perceptions of key issues such as transparency, security, accountability, and privacy. Findings reveal a strong alignment between the LGPD's principles and the ethical values underlying AI. However, important challenges remain, including the absence of specific AI regulation, difficulties related to algorithmic explainability, and uncertainty regarding accountability. The study underscores the urgent need for more robust technical and regulatory frameworks to ensure the responsible development and deployment of AI systems that uphold individuals' fundamental rights.*

Keywords*: LGPD, Artificial Intelligence, Ethics, Data Protection.*

1. Introduction

Ethics, as a branch of philosophy, is concerned with the study of the 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 both individual and collective actions [MacIntyre 2007].

Artificial Intelligence (AI) is a field within computer science focused on developing systems capable of performing tasks that would typically require human intelligence, such as learning, reasoning, decision-making, and interaction with the environment—or processing data at a scale beyond human analytical capacity [Russell and Norvig 2016, Cloud]. Within this context, ethics assumes an important role, given the significant societal impact of this technology. As a disruptive tool, AI has the potential to transform sectors such as healthcare, education, security, and the economy. However, the massive use of data, decision-making autonomy, and the opacity of many algorithmic systems raise major ethical concerns [Floridi et al. 2021]. These concerns include issues such as privacy, fairness, accountability, and transparency, underscoring the need for ethical guidelines to inform the design, implementation, and responsible use of AI technologies [Jobin et al. 2019a, de Cerqueira et al. 2022].

Given this context, this study investigates whether the principles of the Brazilian General Data Protection Law (LGPD)[Rocha et al. 2023] can be effectively mapped to the ethical principles applied to Artificial Intelligence (AI)[de Cerqueira et al. 2021]. To achieve this goal, we conducted a survey with 30 participants—mostly computer science students—through an online questionnaire that assessed their perceptions regarding privacy, transparency, security, and accountability in the use of data by AI systems. In addition, a qualitative and exploratory approach was adopted, combining a literature review, document analysis, and a comparative study. Based on the participants' perceptions, the study provides insights into regulatory challenges and supports the formulation of guidelines that promote the responsible use of AI aligned with individuals' fundamental rights.

2. Background and Related Works

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 [Brasil 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 [Brasil 2019]. According to Article 2 of the LGPD [Brasil 2018], the regulation of personal data protection is grounded in the following principles: I – Respect for privacy; II – Informational self-determination; III – Freedom of expression, information, communication, and opinion; IV – Inviolability of intimacy, honor, and image; V – Economic and technological development and innovation; VI – Free enterprise, free competition, and consumer protection; VII – Human rights, the free development of personality, dignity, and the exercise of citizenship by natural persons. The principles guiding the processing of personal data are outlined in Article 6 of the LGPD. Table 1 presents the LGPD principles [Rocha et al. 2023] considered in this study.

Under the LGPD, the processing of personal data—which includes any operation performed with personal data during its lifecycle—can be carried out by two types of processing agents: 1) **Controller**: Defined by the Law as the natural or legal person, under public or private law, who is responsible for decisions regarding the processing of personal data, such as determining its purposes and means (Art. 5, VI); 2) **Processor**: A natural or legal person, under public or private law, who processes personal data on behalf of the controller (Art. 5, VII), including public agents acting in this capacity, as well as entities distinct from the Controller that process data under a contract or similar instrument. In addition to these agents, there is also the **Data Protection Officer (DPO)**, referred to in Article 5, VIII, as the individual designated by the controller and processor to act as a communication channel between the controller, data subjects, and the National Data Protection Authority (ANPD) [Federal 2021, Brasil 2018].

2.1. Ethical Principles in Artificial Intelligence

Artificial Intelligence (AI) is a field within computer science that aims to develop systems capable of performing tasks that would normally require human intelligence, such as learning, reasoning, decision-making, and interaction with the environment—or tasks involving data at a scale beyond human analytical capacity. These systems rely on advanced algorithms, often based on machine learning and neural networks, to process large volumes of data, identify patterns, make autonomous decisions, categorize

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.

objects, process natural language, generate recommendations, among other capabilities [Russell and Norvig 2016, Cloud]. AI applications have been transforming several sectors—including healthcare, education, industry, and security—bringing significant benefits but also raising important ethical and social challenges [de Cerqueira et al. 2021]. With the advancement and implementation of Artificial Intelligence (AI), the scientific community, legislators, and organizations have emphasized the importance of adhering to ethical principles that guide the responsible development and use of these technologies. Some of the key principles include [UNESCO 2022, Díaz-Rodríguez et al. 2023, de Cerqueira et al. 2021, Floridi et al. 2021, Jobin et al. 2019b, González et al. 2024]:

- **Transparency**: The ability to understand how AI systems make decisions;
- **Privacy**: Respect for privacy and the protection of personal data;
- **Fairness and Non-Discrimination**: AI systems should be designed to avoid bias and discrimination, ensuring that their decisions are fair and equitable;
- **Beneficence and Non-Maleficence**: AI should be used to promote human and social well-being while minimizing risks and harms caused by its implementation;
- **Accountability**: Developers, companies, and users of AI should be held accountable for the impacts of their systems;
- **Human Oversight and Collaboration**: AI should not entirely replace human

supervision and decision-making. It must be used as a collaborative tool that enhances human decision-making;

- **Secure Development**: Cybersecurity is essential in the development of AI systems. These systems should be protected against attacks and vulnerabilities to avoid potential consequences;
- **Fair Distribution of Benefits**: Ensuring that the benefits of AI are distributed fairly across society and not concentrated in the hands of a few.

2.2. Related Works

Several studies have investigated the intersection of ethics, artificial intelligence (AI), and Brazil's General Data Protection Law (LGPD), emphasizing both challenges and opportunities. [Brey and Dainow 2023] proposed a practical approach for embedding ethical principles—such as transparency, accountability, and fairness—into AI system design. [Khan et al. 2023] explored how practitioners and policymakers perceive AI's ethical challenges, highlighting the need for clear regulations and human oversight. [de Cerqueira et al. 2022] introduced the RE4AI Ethical Guide, an interactive tool to support the elicitation of ethical requirements in AI systems, particularly in agile contexts. Developed using Design Science Research, the guide comprises 26 cards structured around 11 ethical principles (based on [Ryan and Stahl 2021]), each featuring explanations, guiding questions, illustrations, and tool suggestions. The guide is implemented as a web-based platform with features such as filtering and card comparison to foster iterative and participatory use. Evaluation with students showed its effectiveness in generating ethical user stories, increasing ethical awareness, and supporting requirements analysis. Contributions include the operationalization of ethical principles in practice, support for documenting ethical decisions, and potential to mitigate ethics washing. Future work includes industry evaluations, NLP-based validation of ethical requirements, and a repository of generated requirements.

Recent studies have examined the interplay between ethics, AI, and LGPD, covering domains such as medicine, cybersecurity, legal theory, and software engineering practice. For instance, [Nascimento et al. 2024] conducted an integrative literature review to map the ethical and legal implications of AI in the medical field. Similarly, [Neves 2023] performed a systematic mapping of the use of AI in clinical practice, emphasizing concerns about data privacy and informed consent. From a broader legal perspective, [Fernandes and MEIRA 2023] reviewed the impact of AI on the Brazilian legal profession, highlighting issues such as the opacity of algorithmic decisions and the need for legal frameworks that address automated reasoning. Building on these discussions, [de Oliveira 2024] analyzed the administrative sanctions established by LGPD's Resolution CD/ANPD nº 4, contributing to the understanding of how Brazil operationalizes data protection enforcement. Complementarily, [Lopes 2023, Frullani Lopes 2021] explored how AI challenges traditional notions of authorship in copyright law, pointing to conceptual and regulatory gaps that arise when machines co-author or autonomously generate content.

Several studies focused on the application and integration of LGPD in technological contexts. [de Araújo Neto and Barbosa Aguiar 2024] reviewed academic and practical works to assess how LGPD has been applied in the field of information security. Likewise, [Rapôso et al. 2019] performed a systematic review over a five-year period to identify trends linking LGPD and information technology, based on sources such as EBSCOhost and Google Scholar. [Sarlet and Ruaro 2021] offered a normative perspective by examining the protection of sensitive personal data in Brazil, outlining the key principles of the LGPD and their implications for technology developers. Ethical concerns surrounding AI development and deployment were a central theme in works such as [Brey and Dainow 2023], which proposed an Ethics by Design approach to embed ethical principles directly into AI system development. The authors grounded their method in qualitative analysis and ethical design models, advocating for the systematic inclusion of values like fairness and accountability from the outset. A theoretical and exploratory lens was adopted by [Rossetti and Angeluci 2021], who discussed the main ethical challenges related to algorithm use in the information society, offering examples of how to navigate ethical dilemmas in practice.

The intersection of AI, ethics, and cybersecurity was also explored in [González et al. 2024], which provided a bibliographic review analyzing both practical applications and ethical consequences in security-sensitive domains. Meanwhile, [Khan et al. 2023] combined a systematic review with empirical data from surveys to explore how professionals and legislators perceive ethical principles and challenges associated with AI, revealing a need for clearer regulation and increased interdisciplinary dialogue. Finally, [Carvalho et al. 2021] contributed an interpretive qualitative study investigating the intersection of ethics, LGPD, and social network analysis (SNA) research in Brazil. Their work underscored the need for ethical awareness in research contexts where data from online social platforms are used, and how LGPD introduces constraints and opportunities for responsible data use. Additionally, [Quintino et al. 2024] examined the ethical implications of using AI to generate scientific texts, employing a PRISMA-based integrative literature review to identify risks such as misinformation and authorship dilution.

3. Research Methodology

Our objective is to investigate the compatibility between ethical principles and those outlined in LGPD within the context of AI. We focus on how these values can be integrated to foster the responsible use of AI. Additionally, we compare the ethical principles commonly associated with AI to the LGPD's guidelines in order to identify areas of convergence and divergence, as well as key ethical and regulatory challenges that emerge in AI implementation. To guide this investigation, we pose the following research questions (RQ):

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

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

To address the research questions, we adopted a qualitative and exploratory approach, combining a literature review, document analysis, and a comparative study. The selected studies were retrieved from the digital databases DBLP computer science bibliography, IEEE Xplore, and Google Scholar.

After selecting the studies, we conducted a literature review, which consisted of a systematic and critical analysis of publications related to the topic.

The goal was to map the current body of knowledge and identify research gaps [Kitchenham and Charters 2007, Petersen et al. 2008]. Following this, we carried out a document analysis, a research technique involving the systematic examination of selected papers to extract relevant information and interpret the data [Petersen et al. 2008]. Finally, we performed a comparative study, an approach used to identify similarities, differences, and patterns between two or more concepts or contexts [Petersen et al. 2008, Armstrong 2012]. During these stages, we analyzed the objectives, methodologies, results, and discussions of each study to gain a deeper understanding of how artificial intelligence is addressed across different fields, how ethical principles are interpreted, and how the LGPD is applied. This process informed the construction of the core questions explored in this article.

3.1. Survey

In order to map how the ethical principles of the LGPD relate to those of Artificial Intelligence, we designed a Google Forms questionnaire and distributed it among computer science student groups to collect participants' opinions on the topic. The questionnaire, available at https://zenodo.org/records/15385394, included an informed consent statement, outlining the conditions of participation in accordance with the ethical standards of privacy established by the LGPD [da República 2018]. Participants were informed that participation was entirely voluntary, with the right to withdraw at any time without penalty. The survey was conducted anonymously, without collecting contact information or any identifiable personal data. Furthermore, all responses were treated with strict confidentiality and used exclusively for academic purposes, ensuring the privacy and protection of the data collected throughout the study.

The questionnaire consisted of sociodemographic questions, such as gender, age, and academic program, as well as questions regarding participants' level of knowledge about the ethical principles of both the LGPD and AI. It also included statements related to LGPD principles, AI principles, and their intersection. To capture participants' perceptions of these statements, we used a Likert scale, a common quantitative method for assessing opinions or attitudes by indicating degrees of agreement or disagreement. In this questionnaire, the scale ranged from 1 to 5, where 1 represented "Strongly Disagree" and 5 represented "Strongly Agree".

4. Survey Results

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 of various other programs. Of these, 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. When it comes to AI principles, only 16.7% claimed to know them, 33.3% knew a little, and 50% had no knowledge (Figure 1).

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

The survey results indicate that participants perceive a strong connection between the ethical principles outlined in LGPD and those guiding the development of ethical AI.

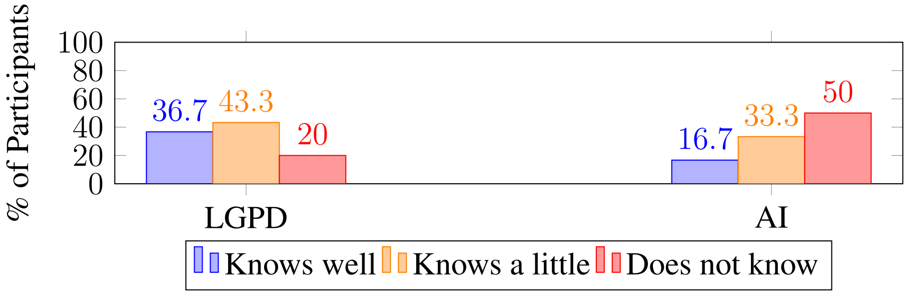

Figure 1. Participants' Knowledge of LGPD and AI Principles

This alignment is particularly evident in areas such as 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 essential aspects for protecting individuals."

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

Among the 30 responses collected, approximately 90% of participants suggested that the principles of the LGPD could serve as a foundation to ensure AI systems respect user privacy, by enforcing clear rules for data collection and use. Transparency also emerged as a key concern, with 90% of participants highlighting that, just as the LGPD requires organizations to inform users about how their data is processed, AI systems should incorporate algorithmic explainability to ensure automated decisions are understandable (Figure 2). In addition, around 76.7% of respondents emphasized the importance of data minimization and security—central tenets of the LGPD—arguing that AI should avoid excessive data collection and adopt strict safeguards to protect user information.

Information security was identified as a shared concern, underscoring the need for robust mechanisms to protect both stored data and the automated decision-making processes (Figure 2). Finally, about 40% of participants agreed that AI developers should be accountable for the outcomes of automated decisions, aligning with the LGPD's principle of accountability. These findings suggest that future AI regulation may benefit from adopting a similar framework to the LGPD, ensuring governance and audit mechanisms are in place to oversee data usage (Figure 2).

RQ.1 Summary: Participants associated LGPD principles with AI ethics, highlighting privacy, transparency, data minimization, and accountability as key overlaps. Most agreed that LGPD can guide ethical AI development through clear data use rules and explainability.

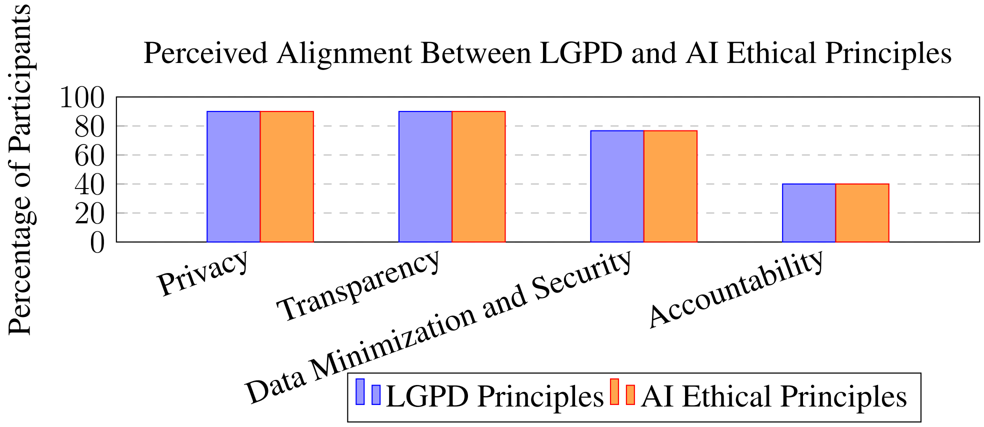

Figure 2. Participants' perceptions of alignment between LGPD principles and ethical principles in AI.

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

As previously introduced, the integration of LGPD principles into AI development poses significant ethical and technical challenges. Although 86.7% of participants believe that explicit consent should be required before any organization collects and uses personal data, AI systems often rely on continuous learning processes that make it difficult to trace and maintain consent over time. One potential solution is the implementation of dynamic consent management mechanisms, which would allow users to update or withdraw data usage permissions as needed (Figure 3). Regarding data security, approximately 50% of respondents believe that protecting personal data should be a high priority for companies. However, several responses expressed concern about the practical enforcement of this principle, especially given the large volumes of data processed by AI systems. This increases the risk of sensitive data leaks and cyberattacks. Addressing this challenge may require the adoption of robust security measures, such as encryption, anonymization, and compliance with strong data protection protocols, as required by the LGPD (Figure 3).

In terms of accountability, only 40% of participants agreed that AI developers should be held responsible for the impacts of decisions made by AI systems. This indicates a degree of uncertainty around who should be liable when automated systems cause harm or errors. While the LGPD promotes the principle of accountability, AI systems often operate autonomously, making it difficult to clearly assign responsibility. A possible solution is the development of specific regulations that define legal responsibilities for developers and organizations, ensuring oversight of automated decision-making processes (Figure 3). Finally, only 43.3% of participants believe that AI algorithms should be explainable and understandable to users. This reflects a limited expectation for algorithmic transparency, despite the importance of this issue. The opaque nature of many AI systems can lead to risks in the processing of personal data and hinder auditing processes. Investing in explainable AI (XAI) is a promising approach to ensure that users understand how their data is being used and have the ability to challenge or contest automated decisions (Figure 3).

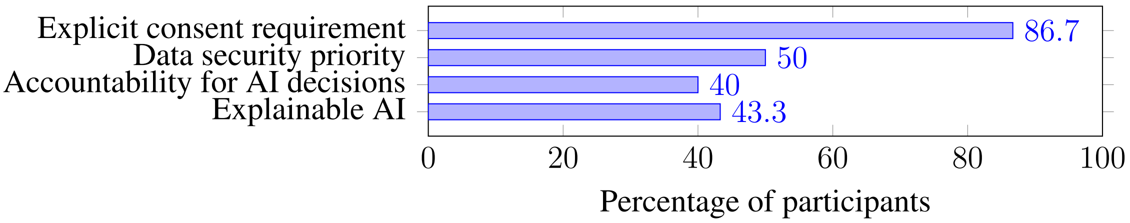

Figure 3. Participant agreement with key ethical principles and challenges in applying LGPD to AI (N=30).

RQ.2 Summary: Participants highlighted challenges in applying LGPD principles to AI, including ensuring explicit consent in continuous learning systems, enforcing data security at scale, defining accountability for AI decisions, and improving algorithmic transparency. Proposed solutions include dynamic consent management, robust encryption, legal responsibility frameworks, and investments in explainable AI.

5. Limitations and Threats to Validity

Despite the relevance of the research, some limitations and threats to its validity should be considered. Among the limitations, we can highlight: 1) Limited sample: The study was conducted with a limited number of participants (30 students) from computing courses only, which prevents generalizing the findings to the broader population or other contexts; 2) Lack of advanced statistical analysis: The research does not employ more robust statistical techniques (such as correlation tests), which could have provided a more precise assessment of the relationships between variables and strengthened the conclusions; and 3) Focus on theoretical aspects only: The study does not delve deeply into practical examples or real-world case studies, which could enrich the understanding of the challenges and proposed solutions.

The threats to validity were analyzed across the dimensions of internal, construct, conclusion, and external validity [Wohlin et al. 2012]. In this context, the following threats can be identified: **Internal validity**: The research exhibits selection bias due to the sample being restricted to computing students, limiting its representativeness. There is also a self-report bias, as participants may provide socially desirable responses instead of genuine ones. Additionally, the use of the Likert scale may be a limitation, as it does not fully capture the complexity of participants' opinions. **Construct validity**: There is some ambiguity in the survey statements, which could lead to different interpretations by participants, compromising the accuracy of their responses. Furthermore, the lack of proper context in the questions may hinder a deeper understanding of the principles being addressed. **Conclusion validity**: The generalization of the results is limited due to the small and specific sample, making it difficult to extrapolate findings to larger populations. The data analysis may also be considered superficial, as the small number of responses could affect the robustness of the conclusions drawn. **External validity**: The sample is not representative of groups outside the computing student population, which prevents the generalization of results to other audiences. Additionally, the lack of diversity in the sample limits the breadth of the conclusions, which may not reflect the perceptions of individuals from various social and professional backgrounds.

6. Conclusion and Future Work

This study explored the relationship between the principles of LGPD and the ethical principles of Artificial Intelligence, identifying both synergies and challenges in applying these guidelines. The results show a strong alignment on privacy, transparency, security, and accountability, but highlight practical implementation challenges, such as the lack of specific AI regulations and issues with algorithm explainability. While the LGPD could serve as a foundation for ensuring data protection in AI, its application still faces technical and legal hurdles. A major concern raised by participants was the lack of clarity regarding accountability in automated systems, emphasizing the need for more detailed regulations. Key challenges identified include ensuring explicit consent in continuous learning systems, safeguarding large-scale data, and establishing effective mechanisms for auditing automated decisions. The study also highlighted the need for investment in explainable AI, enabling users to understand how their data is used and providing ways to contest automated decisions. Future work should expand the sample to include legal experts and industry professionals, and conduct empirical studies to assess the application of LGPD in real-world AI use cases. Research aimed at developing more effective regulatory and technical mechanisms could contribute to a stronger integration of data protection and algorithmic ethics, ensuring more responsible AI use.

Data Availability

The data that support the findings of this study are openly available in Zenodo at https://zenodo.org/records/15385394.

Acknowledge

This study was financed in part by the Project No. 514/2023 – Call Nº 10/2023 – FAPDF Learning Program, a strategic development initiative in the macro areas of Agro Learning, Bio Learning, Gov Learning, and Tech Learning.

References

Armstrong, K. (2012). Methods in comparative effectiveness research. *Journal of clinical oncology*, 30(34):4208–4214.

Brasil (2018). Lei nº 13.709, de 14 de agosto de 2018 - lei de proteção geral de dados. Disponível em `https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm` (Janeiro 2025).

Brasil (2019). Lei nº 13.853, de 8 de julho de 2019 - lei de proteção geral de dados. Disponível em `https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm` (Janeiro 2025).

Brey, P. and Dainow, B. (2023). Ethics by design for artificial intelligence. *AI and Ethics*, pages 1–13.

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.

Cloud, G. O que é inteligência artificial (ia)? Disponível em `https://cloud.google.com/learn/what-is-artificial-intelligence` (Janeiro 2025).

da República, Presidência, N. C. (2018). Brazilian general data protection law (lgpd). *Nartional Congress, accessed in April 10, 2022*, 1(1):1–31.

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).

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.

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 Araújo, R. D., Dorça, F. A., de Araujo, R. M., Siqueira, S. W. M., and Fontão, A. L., editors, *SBSI 2021: XVII Brazilian Symposium on Information Systems, Uberlândia, Brazil, June 7 - 10, 2021*, pages 36:1–36:8. ACM.

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.

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.

Federal, G. (2021). Guia de boas práticas para implementação na administração pública federal. 2020.

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).

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.

Frullani Lopes, M. (2021). Obras geradas por inteligência artificial: desafios ao conceito jurídico de autoria (works generated by artificial intelligence: Challenges to the legal concept of authorship). *Available at SSRN 3874667*.

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.

Jobin, A., Ienca, M., and Vayena, E. (2019a). The global landscape of ai ethics guidelines. *Nature machine intelligence*, 1(9):389–399.

Jobin, A., Ienca, M., and Vayena, E. (2019b). The global landscape of ai ethics guidelines. *Nature machine intelligence*, 1(9):389–399.

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.

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

Lopes, M. F. (2023). *Obras geradas por inteligência artificial: desafios ao conceito jurídico de autoria*. Editora Dialética.

MacIntyre, A. (2007). *After virtue: A study in moral theory*. University of Notre Dame Pess.

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.

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.

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)*. BCS Learning & Development.

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*.

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.

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 Hong, J., Lanperne, M., Park, J. W., Cerný, T., and Shahriar, H., editors, *Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing, SAC 2023, Tallinn, Estonia, March 27-31, 2023*, pages 1352–1361. ACM.

Rossetti, R. and Angeluci, A. (2021). Ética algorítmica: questões e desafios éticos do avanço tecnológico da sociedade da informação. *Galáxia (São Paulo)*, (46):e50301.

Russell, S. J. and Norvig, P. (2016). *Artificial intelligence: a modern approach*. Pearson.

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.

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.

UNESCO (2022). Recomendação sobre a Ética da inteligência artificial. Disponível em https://unesdoc.unesco.org/ark:/48223/pf0000381137_por (Janeiro 2025).

Wohlin, C., Runeson, P., Höst, M., Ohlsson, M. C., Regnell, B., Wesslén, A., et al. (2012). *Experimentation in software engineering*, volume 236. Springer.