Journal of Internet Services and Applications, 2025, 16:1, doi: 10.5753/jisa.2025.5247

Optimizing Compliance: Comparative Study of Data Laws and Privacy Frameworks

Lucas Dalle Rocha [**University of Brasília (UnB); Aalto University** | ***lucas.rocha@aalto.fi***]
Edna Dias Canedo [**University of Brasília (UnB)** | ***ednacanedo@unb.br***]

University of Brasília (UnB), Brasília, DF, 70910-900.

Received: 30 November 2024 • **Accepted:** 12 May 2025 • **Published:** 20 July 2025

Abstract Regarding privacy laws and digital globalization, understanding data regulation compliance and cross-jurisdictional challenges remains limited. To avoid administrative sanctions and protect user data, organizations and developers must bridge these gaps, navigating laws such as the General Data Protection Regulation (GDPR), the American Data Privacy and Protection Act (ADPPA), the General Data Protection Law (LGPD), and the Australian Privacy Act. This study focuses on creating a comprehensive compliance tool by investigating the similarities and nuances of these laws, as well as the challenges developers and organizations face in implementing Privacy by Design principles and ISO/IEC 29100 standards. Through a Systematic Literature Review (SLR) approach, topics of convergence and divergence among privacy laws and frameworks were pinpointed, as well as the challenges of implementing these laws in software. A survey was used to validate the challenges found in the SLR in the Brazilian context, in which most participants demonstrated a lack of knowledge regarding the LGPD. Lastly, we applied Framework Analysis to code and index key legislation points, allowing us to correlate them and develop a compliance-assistance tool. In the several contributions achieved, there is a deeper understanding of the privacy implications in a global context and its practical challenges, and also a practical guidance development, translating legal requirements into actions. Some limitations in this study lie in the interaction between selection and treatment in the survey, as participants' responses will not necessarily serve to generalize the challenges faced by all developers and organizations. In general, the contributions offer valuable theoretical and practical insights in the field of data privacy.

Keywords: Data Privacy, Privacy Requirements, Privacy Challenges, General Data Protection Law, Privacy by Design, ISO/IEC 29100, Privacy Frameworks.

1 Introduction

Since the period before Industry 4.0, technological advances have progressively corroborated data migration from physical to digital media; therefore, a massive amount of information is stored daily on local servers and in the cloud [Selim, 2021]. Additionally, in a digital environment, it is customary to transfer files that contain data stored in their structure — commonly known as metadata —, such as texts, images, videos, etc., since they only occupy a small amount of memory space relative to the content stored [Feng *et al.*, 2018]. This fact corroborates the intensification of digital media as opposed to physical media. However, inadequate handling of personal data, as evidenced by major information leaks in Brazil, highlights the critical need for compliance with privacy laws, especially regarding sensitive information [Cambraia, 2021].

In the legal sphere, the Brazilian data privacy law, known as the General Data Protection Law (LGPD) [Brasil, 2018], establishes a series of principles aimed at guaranteeing the privacy of individuals, including its extraterritorial applicability. That means it is applied to organizations outside Brazil that handle personal data of Brazilian citizens [Brasil, 2018]. However, these principles are an abstraction with little technicality observed in a world of multiple data privacy laws [Sangaroonsilp *et al.*, 2023]. In that way, it is not enough to comply only with national or regional privacy laws. Still, it is essential to know which laws are commonly practiced and to resolve, where appropriate, the dilemmas between them. That said, companies must rely on specific guides or methodologies to guarantee privacy compliance, but on the other hand, there is almost never a consensus when it comes to handling international data across multiple privacy laws [Sangaroonsilp *et al.*, 2023].

Finally, integrating international and national legislation is essential for organizations that handle personal data, ensuring compliance and resilience in the face of potential violations [Sirur *et al.*, 2018]. In the face of the increasing digitization and sharing of documents, some developers involved in data processing still don't know how to translate laws, such as the LGPD, into a technical context, which reflects a lack of knowledge about the methods needed to ensure compliance with the principles of this law [Sangaroonsilp *et al.*, 2023], [Ekambaranathan *et al.*, 2023], [Machado *et al.*, 2023], [Davier *et al.*, 2023], [Canedo *et al.*, 2022]. Furthermore, it is essential to understand as many local privacy laws as possible, especially in international contexts, to avoid inappropriate processing of personal data [Machado *et al.*, 2023]. This work will investigate the nuances between data privacy laws and frameworks used in various countries through a comparison with the LGPD while proposing unified solutions for developers and organizations to build a privacy-compliant digital environment.

Given the rapid migration of information to the virtual environment [Carvalho *et al.*, 2020], the exposure of personal data has become a critical issue, as privacy violations go against what is explained by the LGPD [Brasil, 2018]. In addition, it is not enough to comply only with local legislation since some laws can act extraterritorially [Hornuf *et al.*, 2023]. This paper aims to compare the LGPD with international legislation and frameworks to explore the challenges in international data sharing, proposing practical and unified solutions to ensure compliance with multiple laws. The choice of legislation is based on international relevance and a preference for countries with Portuguese or English as their official native language, including the LGPD, the General Data Protection Regulation (GDPR), the Australian Privacy Act, and the American Data Privacy and Protection Act (ADPPA). At the same time, the selected frameworks are Privacy by Design (PbD) and ISO/IEC 29100, which directly inspired the creation of the European law [Barth *et al.*, 2023] and corroborate the implementation of privacy in software.

The main goal is to assist professionals in selecting privacy frameworks, given the coverage of the laws. To this end, the research explores the similarities and differences in the data protection laws of these countries. It verifies how the frameworks align with the laws to support the implementation of protection standards for personal data. The study will also investigate the perception of developers and organizations about compliance with the LGPD by identifying how organizations can apply privacy frameworks to meet legal requirements, cataloging the techniques used and the challenges faced by organizations and proposing a guide to help implement unified solutions for compliance with privacy laws.

The motivation for this work is a secure digital environment that complies with privacy laws, not only protecting individual data but also strengthening public trust and providing a solid foundation for business growth and innovation [Canedo *et al.*, 2022]. Consequently, by providing practical and unified solutions for compliance with multiple data protection laws, this study will contribute to creating a culture of privacy that benefits both organizations, their developers, and end users.

2 Background and Related Work

Firstly, it is essential to understand how data are divided and understood by the law since the process of data anonymization is, in its rudimentary form, a conversion between these types of data. The LGPD defines, in Art. 5° (I-III), three types of data and their following concepts [Brasil, 2018]: 1) Personal data: information relating to an identified or identifiable natural person; 2) Sensitive personal data: personal data on racial or ethnic origin, religious conviction, political opinion, membership of a trade union or religious, philosophical or political organization, data relating to health or sex life, genetic or biometric data, when linked to a natural person; and 3) Anonymized data: data relating to a data subject who cannot be identified, taking into account the use of reasonable technical means available at the time of processing.

It should be noted that once the data have been anonymized, it is no longer legally covered by the LGPD [Doneda, 2020]. This means that data controllers have the legal backing to operate on this information without sanctions being applied in the event of noncompliance since it is no longer personal data. It is also worth noting that the other data privacy laws also have similar concepts regarding types of data, which will be compared later using the framework analysis technique [Goldsmith, 2021]. The LGPD defines the entities involved in the processing of personal data in Art. 5° (VI-VIII) [Brasil, 2018]: 1) Controller: natural or legal person, governed by public or private law, who is responsible for decisions regarding the processing of personal data; 2) Operator: natural or legal person, governed by public or private law, who carries out the processing of personal data on behalf of the controller; and 3) Data Protection Officer (DPO): a person appointed by the controller and operator to act as a communication channel between the controller, the data subjects, and the National Data Protection Authority (ANPD).

The concepts presented for the LGPD are valid and correlatable for most legislation, for example, the direct equivalence of definition concerning the entities involved in processing personal data from the GDPR (controller and processor) [European Parliament and Council, 2018]. Regarding the sections to be discussed, the scope of application of the laws is divided into: personal scope (extent to which individuals personal data are covered by privacy laws and regulations); territorial scope (geographical boundaries within which data protection laws apply); and material scope (specific types of data or activities that fall under the jurisdiction of data protection laws).

There are two relevant concepts for personal scope: opt-in consent (mandates every participant to knowingly agree to the construction or processing of his/her data) and opt-out consent (enables organizations to carry out the personal data collection and processing by default). In addition, a good starting point for translating a law into a technical context is to identify the principles that are ideals addressed by the law in an abstract and simple way and to introduce the fundamental rights to be respected [Neves, 2021]. The LGPD presents ten guiding principles to guarantee data protection in Art. 6° [Brasil, 2018].

Before the main privacy laws were formulated, the guidelines — focused on developers — for protecting personal data were mostly established by privacy frameworks by design [Barth *et al.*, 2023]. The idea is that, by means of basic principles made explicit at a high level (as in legislation), professionals involved in the design and development of software can be guided toward privacy awareness [Barth *et al.*, 2023]. Therefore, since many of these principles are still being put into practice, it is necessary to understand these frameworks, as they can help developers translate laws into a technical context [Sangaroonsilp *et al.*, 2023].

Firstly, there is Privacy by Design (PbD), proposed by Ann Cavoukian in 2009, which advocates the integration of privacy from the start of software development. Based on seven global principles, PbD facilitates the implementation of privacy measures throughout the software lifecycle [Cavoukian, 2009]. Its application makes it possible to align the individual rights of legislation with development practices, guaranteeing protection since the early stages of software development [Aljeraisy *et al.*, 2022a]. In addition, ISO/IEC 29100, developed by ISO in 2011 and updated in 2020, establishes principles for the treatment of Personally Identifiable Information (PII). The framework defines guidelines that align with concepts present in LGPD and GDPR, such as sensitive data, anonymization, and consent [ISO Central Secretary, 2011]. With a comprehensive scope, it applies to organizations of different sizes, helping to translate legal requirements into technical practices, from the specification to the maintenance of systems [Barth *et al.*, 2023].

2.1 Related Work

Aljeraisy *et al.* [2022b] conducted a comparative study of five privacy laws in regions where English is the main language: the European Union, Canada, California, Australia, and New Zealand. Each guideline's key principles and individual rights were identified, and the framework analysis method was applied to perform a comparative analysis. Despite this, the study does not include the LGPD and focuses only on principles and individual rights, so it does not deal with scope, definitions, and respective sanctions.

In order to analyze not only privacy legislation but also frameworks, Barth *et al.* [2023] sought to unify the guidelines available to developers by codifying attributes identified in multiple laws and frameworks. In addition to investigating the principles of various laws, such as Australian and European, the work addresses the PbD principles and, similarly, those of ISO/IEC 29100, in order to identify their similarities with legislation and propose recommendations for developers in sometimes contradictory situations when it comes to guidelines. However, despite bringing together fourteen guidelines and codifying them into a common solution, there is no mention of Brazilian law.

The study proposed by Canedo *et al.* [2022] sought to understand the perception of agile teams in the process of adapting to LGPD, i.e., what changes were necessary (both in procedures and in teams) to ensure compliance with LGPD. Through an SLR, survey application, and data triangulation, the work identified various challenges pointed out by IT professionals, ranging from the organization's infrastructure — such as the lack of a data security and privacy policy — to implementation difficulties, such as the lack of a guide or tool that could help with the elicitation of privacy requirements. In this way, the study deals with the gradual evolution of compliance in relation to each principle of Brazilian legislation.

In order to establish an in-depth comparison between privacy laws, Sangaroonsilp *et al.* [2023] developed a taxonomy focused on four privacy laws and frameworks: the GDPR, ISO/IEC 29100, Thailand's Personal Data Protection Act, and the Asia-Pacific Economic Cooperation framework. To do this, the requirements of the guidelines are extracted and refined so that they can be analyzed semantically and classified according to their similarities and differences. Despite GDPR and ISO/IEC 29100, the study is based on legislation and frameworks from the Asian continent, i.e., it does not address Brazilian, American, or Australian laws.

The study by Canedo *et al.* [2020] identified, through a systematic review of the literature, various models and techniques that developers use to implement privacy in software, in addition to elucidating through qualitative research how professionals in information and communication technology understand LGPD. The work not only identifies specific challenges for developers — for example, insufficient knowledge and interference from the organizational environment — but also presents a comparative table between the principles of the LGPD and the GDPR since they are essentially similar to those of ISO/IEC 29100. Thus, the principles and some individual rights are elucidated, although this is not its primary focus.

Camêlo and Alves [2023] have implemented a privacy standard catalog, which brings together aspects of the LGPD, the PbD, and ISO/IEC 27701 in order to facilitate the LGPD compliance process for developers. In addition to explaining tasks related to data processing, such as access to information and the collection of personal data, a guide is proposed to help developers in the process of implementing privacy in software. However, the study focuses only on Brazilian legislation, and when it comes to cross-border data handling, the other various guidelines involved must be taken into account.

In that way, there are different approaches regarding prior work, such as merely comparing legislation (at various levels), only presenting the organizational challenges in complying with the laws, or both. Table 1 elucidates the main differences between this work and the related works.

Concept	Aljeraisy *et al.* [2022b]	Machado *et al.* [2023]	Li *et al.* [2022]	Barth *et al.* [2023]	Canedo *et al.* [2020]	Sangaroonsilp *et al.* [2023]	Camêlo and Alves [2023]	Canedo *et al.* [2022]	Ferrão *et al.* [2024]	**This study**
LGPD					x		x	x	x	x
GDPR	x	x	x	x	x	x	x	x	x	x
ADPPA										x
Australian Privacy Act	x			x						x
Privacy by Design	x	x		x	x		x			x
ISO/IEC 29100				x	x	x		x	x	x
Comparison Between Laws	x			x	x	x		x	x	x
Organizational Challenges	x	x	x		x	x	x	x		x

Table 1. Comparison between related works and the proposed study.

Our findings made it possible to draw up a practical and accessible guide for professionals in the field, thus complementing previous studies that present comparisons between legislation and specific challenges. For example, studies such as Canedo *et al.* [2020], Sangaroonsilp *et al.* [2023], and Canedo *et al.* [2022] discuss both comparisons between laws and the challenges faced by organizations. However, these studies only focus on one aspect of legislation (such as principles or rights), without delving into compliance techniques or the integration of multiple frameworks.

In addition, studies such as Aljeraisy *et al.* [2022b], Barth *et al.* [2023], and Camêlo and Alves [2023] are much more in line with the proposal of this work, in terms of comparison, since they use coding techniques to map requirements. However, the current work differs in that it explores scope, definitions, and sanctions addressed by laws and integrates

Privacy by Design practices and the ISO framework. In this way, the guide seeks to meet the specific needs of developers and their respective organizations by providing practical and detailed guidelines for achieving compliance effectively and interactively.

3 Research Design

This study employs exploratory research, including a bibliographical survey comparing legislation and frameworks, an SLR to identify challenges faced by organizations, and explanatory research using a survey to collect information regarding the difficulties. The SLR is based on Kitchenham *et al.* [2007] guidelines and is supplemented by the snowball technique to identify a comprehensive collection of relevant studies and to refine the research questions [Felizardo *et al.*, 2016]. **Figure 1** shows the research methodology, while specific information about each stage can be found at Zenodo[1] [Rocha and Canedo, 2024].

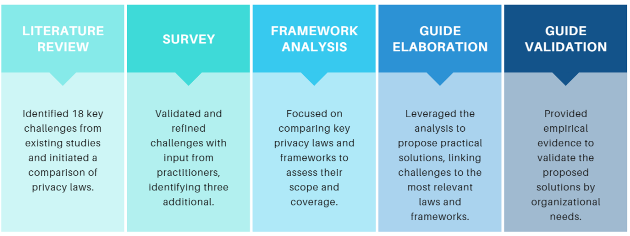

LITERATURE REVIEW
SURVEY
FRAMEWORK ANALYSIS
GUIDE ELABORATION
GUIDE VALIDATION
Identified 18 key challenges from existing studies and initiated a comparison of privacy laws.
Validated and refined challenges with input from practitioners, identifying three additional.
Focused on comparing key privacy laws and frameworks to assess their scope and coverage.
Leveraged the analysis to propose practical solutions, linking challenges to the most relevant laws and frameworks.
Provided empirical evidence to validate the proposed solutions by organizational needs.

Figure 1. Steps to carry out this research.

Additionally, the methodology is enhanced with a framework analysis method to address gaps not identified in the SLR. This method is structured in five key stages: (1) Data Familiarization, (2) Framework Identification, (3) Indexing, (4) Charting, and (5) Mapping and Interpretation [Goldsmith, 2021]. Surveys were analyzed using a qualitative approach — with an emphasis on grounded theory to categorize open-ended responses [Chun Tie *et al.*, 2019] — to infer the challenges and solutions related to applying laws in organizations. The combined methods ensure a practical analysis: while the SLR and the Framework Analysis cover the state of the art, the survey allows for empirical validation, ensuring that the guide is produced to its highest standards. In that way, the research questions (RQ) that will guide this study are as follows:

RQ.1: **What are the main points of similarity and difference between the data protection laws of Brazil, the European Union, the USA, and Australia?**
This question aims to carry out a comparative analysis of data protection laws regarding these laws, identifying key similarities and differences to develop a comprehensive data protection approach in a globalized context.

RQ.2: **What are the challenges and techniques faced by organizations and developers when adapting to data protection laws in Brazil, the European Union, the USA and Australia?**
This RQ aims to investigate the practical challenges and adaptation techniques that permeate organizations.

3.1 Search Strategy

The search string was designed around four components: legislation name, comparison type, expected results, and study purpose. The generic string was established as follows:

(“LGPD” OR “GDPR” OR “ADPPA” OR “Privacy Act” OR “General Data Protection Law” OR “General Data Protection Regulation” OR “American Data Privacy” OR “Privacy Amendment Act of 2012”) AND (“Comparison” OR “Similarities” OR “Differences”) AND (“Challenges” OR “Opportunities”) AND (“Compliance” OR “Regulation”)

The digital databases chosen to run the search string were: ACM Digital Library, IEEE Xplore, Scopus, and dblp: computer science bibliography. In the article selection stage, two researchers initially selected the papers independently. At the end of each iteration of the snowball process, a meeting was held to decide on the differences. Papers were only included if both researchers agreed; otherwise, they were excluded.

The inclusion criteria were the following: **(IC1)** Studies must be published as full-paper articles; **(IC2)** Studies must specifically address one of the following current data protection laws: Brazilian, European, US, or Australian; **(IC3)** Studies must highlight the challenges faced by organizations when seeking compliance with data protection laws in Brazil, the European Union, the USA, or Australia; **(IC4)** Studies must be published in Portuguese or English; and **(IC5)** Studies must have been published from 2018 onward, specifically between 2018 and 2024.

Also, the exclusion criteria were the following: **(EC1)** Studies that are not available in full text in the digital databases used should not be included; **(EC2)** Studies that focus exclusively on frameworks, without addressing the desired data protection laws, should not be included; **(EC3)** Studies that, while addressing one of the laws, do not focus on aspects other than the legislation itself as the main subject of study should not be included; and **(EC4)** Studies that do not present legal comparisons between laws — where the laws are only explained without providing comparative analysis — or that present challenges outside the scope of software engineering, should not be included.

3.2 Data Extraction

A spreadsheet with categorized columns was created to categorize study details, such as study ID, title, authors, journal/conference name, and publication date. In addition, several other columns with information on the studies were structured and are available at Zenodo [Rocha and Canedo, 2024]. **Figure 2** shows the initial stages of study selection, resulting in the selection of 15 studies.

Meanwhile, **Figure 3** shows the iterations of the snowball (backward and forward), as well as the number of articles

[1] `https://doi.org/10.5281/zenodo.14172394`

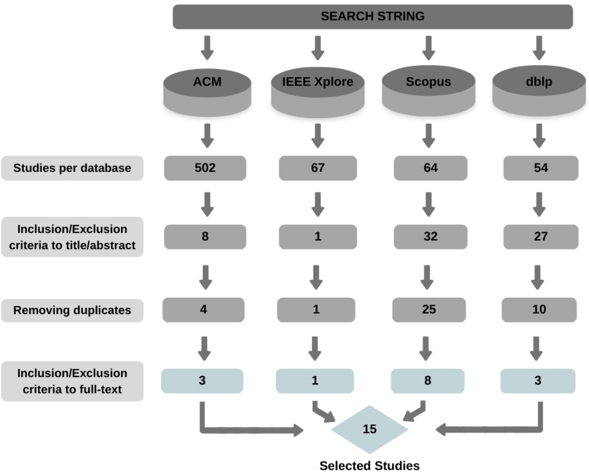


Figure 2. Initial stages of the SLR.

selected up to the saturation point. The backward snowball technique is trivial, as all that is needed is to read the article's references and apply the selection criteria. For the forward snowball, Google Scholar was used, by also applying the selection criteria to all the new studies identified. Consequently, a total of 53 studies were selected (more than three times the number initially established), and each one was read in full.

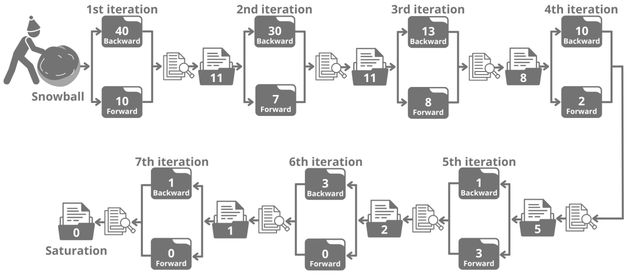


Figure 3. Studies selected after each snowball iteration.

In the data extraction phase, three researchers independently populated the spreadsheet. In the event of disagreement, weekly meetings were held, which even prompted the creation and maintenance of new categories. The process also involved the participation of a professional in privacy laws so that it could be better aligned with the relevant categories for evaluating the laws. At the end of the extraction, the spreadsheet had 53 rows (one for each study) and columns filled in for each piece of information (and gaps, in case of missing data). The list of accepted studies, along with the responses to the RQs and detailed information on the 18 challenges, can also be found in Zenodo [Rocha and Canedo, 2024].

3.3 Survey Methodology

The survey was developed using the Google Forms platform and took approximately 8 minutes to complete. Initially, participants were individually invited via the LinkedIn platform in order to prioritize the selection of participants who work in the software development area and were familiar with the LGPD. The respondents were informed that participation was anonymous, voluntary, and purely for research purposes, so they had to consent to participate in the survey.

The survey questionnaire included 12 questions focused on participants' profiles and the challenges they face with respect to their organization and the LGPD. These questions were organized as follows [Rocha and Canedo, 2024]: Questions Q1 to Q7 approached participants' background, demographics, area of activity, and professional experience; Question Q8 sought to validate the results obtained in the SLR regarding developer challenges; Questions Q9 to Q12 were open-ended and participants could state the biggest compliance challenges and mitigation techniques, so grounded theory was applied to categorize them (see **Table 2**).

Table 2. Survey questions related to participants' profiles and challenges.

ID	Question
Q1	What is your age?
Q2	Which state do you live in?
Q3	What is your level of education?
Q4	In which stage of software development do you work professionally?
Q5	What is the nature of the organization you work for?
Q6	How long have you been working in software development?
Q7	With regard to data privacy, are you familiar with the General Data Protection Law (LGPD)?
Q8	Check which of the challenges listed below you face in your organization to ensure compliance with privacy legislation.
Q9	In your opinion, what are the biggest challenges in implementing the principles of the LGPD during software development?
Q10	In your opinion, what are the best techniques/practices that guarantee the privacy and data protection required by the LGPD?
Q11	Can you describe in detail how your team mitigates the challenges of complying with the LGPD?
Q12	If you have anything to add, please use this question.

The survey was available online for five weeks and collected 122 responses. Also, a copy of the survey diagram — in addition to the answers discussed later — can be found on Zenodo [Rocha and Canedo, 2024].

4 Results

4.1 RQ.1: What are the main points of similarity and difference between the data protection laws of Brazil, the European Union, the USA and Australia?

The studies present the most diverse points of convergence and divergence, dealing with the scope of the law, identifying personal data and the parties involved in processing, the specific legal definitions of each law, individual rights, principles, and, as a consequence of noncompliance, penalties. Studies related to GDPR can be easily found, including comparisons with LGPD itself. The biggest obstacle was identifying studies that related American legislation, the ADPPA, to others since it is the most recent of the objects of study in this work. To meet this need, results on California's privacy law — the California Consumer Privacy Act (CCPA) — were also extracted, given their legal and regional similarities. **Table 3** shows the comparisons split by theme after applying the Framework Analysis. In addition, the process can be seen step by step, including the gaps after SLR, on the Zenodo platform [Rocha and Canedo, 2024].

With regard to the scope of coverage, a similarity between the LGPD and the GDPR is the opt-in-oriented consent; that is, data subjects make it clear that they accept the processing before it begins, and it is considered an individual right [Canedo *et al.*, 2021a], [Canedo *et al.*, 2022]. In contrast, the CCPA adopts opt-out consent, in which consent is considered by default, creating a divergence between Brazilian and European law [Voss, 2021], [Park, 2019].

While European and Brazilian legislation prioritizes the individual's privacy rights, US and Canadian laws focus more on corporative freedom, especially concerning employee data. For example, the ADPPA does not cover employee data, unlike the GDPR and LGPD [Sangaroonsilp *et al.*, 2023], [Kaufmann *et al.*, 2022], [Naqvi and Batool, 2023], [Matulytė, 2022].

When it comes to territorial scope, LGPD and GDPR have similar actions in that even if the organizations are not physically located in their respective territories; the legislation may still be applicable, requiring only that they process citizens' data [Canedo *et al.*, 2022], [Li *et al.*, 2022]. In this way, the GDPR offers greater regulatory autonomy than other data privacy laws due to its more mature legal framework [Lorenzon, 2021], [Weber *et al.*, 2020].

All laws have a special category that defines sensitive personal data [Kaufmann *et al.*, 2022], [Canedo *et al.*, 2021b], [Rocha *et al.*, 2023], [Anwar *et al.*, 2018], which is a mark of similarity, and their definitions are similar, such as racial or ethnic origin, political opinion, and health data. However, ADPPA is more detailed than GDPR and LGPD [Kaufmann *et al.*, 2022]. A point of divergence between the GDPR and the LGPD is that the first considers data that indirectly identify an individual to be sensitive, while the latter requires direct identification [Canedo *et al.*, 2021b]. Finally, a key differentiating point of Australian law is that it considers an opinion about an individual to be personal data.

Most laws — with the exception of Australian law — specify entities responsible for processing personal data [Sangaroonsilp *et al.*, 2023], [Ardabili *et al.*, 2022], [Daoudagh and Marchetti, 2022], [Kaufmann *et al.*, 2022], [de Castro *et al.*, 2022] and, in addition, identify them by classes such as operator, controller, the person in charge — Data Protection Officer (DPO) in the GDPR [Davier *et al.*, 2023], [Poritskiy *et al.*, 2019] —, processor, etc.

As discussed above, the GDPR also offers broader coverage of individuals than CCPA and ADPPA, as ADPPA only applies to US residents and CCPA only applies when it comes to financial transactions. At the same time, the GDPR covers all EU citizens [Wong *et al.*, 2023], [Kaufmann *et al.*, 2022], [Almeida *et al.*, 2022], [Naqvi and Batool, 2023]. In addition to that, Australian law has the least coverage [Anwar *et al.*, 2018], and with regard to children, the CCPA allows consent as young as 13, while the GDPR does not [Alomar and Egelman, 2022].

Regarding the life cycle of personal data, there are some notable similarities and differences between the GDPR, the CCPA, and the ADPPA [Ardabili *et al.*, 2022]: the collection is minimized in the European and North American laws, but is more flexible in CCPA (it is enough to notify the holders); transfer is different in the three laws since it is oriented to the user's objection in the GDPR, allowed by de-identified data in the ADPPA and allowed merely by prior notice in the CCPA; processing is similar in the GDPR and ADPPA, only consistent with the purposes, while in the CCPA only pseudonymization is required; and retention differs, such that it is consistent with the purposes in the GDPR, as a rule at the end of the service or when required by law in the ADPPA and based on the user's request in the CCPA (despite having a clear right to deletion [Park, 2019]), which again highlights the opt-out process.

The GDPR and LGPD share many individual rights and principles [Canedo *et al.*, 2021a], [Canedo *et al.*, 2022], but the GDPR does not have direct equivalence for some LGPD principles, such as open access, prevention and non-discrimination, which are treated as individual rights in European law [Canedo *et al.*, 2020], [Neves, 2021]. Likewise, Australian legislation establishes rights similar to GDPR [Aljeraisy *et al.*, 2022b], but does not present rights to restrict processing, data portability, or to oppose automated decision making, despite considering anonymization as a principle, opposed to GDPR and LGPD [Aljeraisy *et al.*, 2022b].

Finally, penalties vary between the laws since the GDPR can impose fines of up to 20 million euros or 4% of an organization's global turnover, while the CCPA fines each violation individually, with damages ranging from 100 to 750 dollars [Wong *et al.*, 2023]. Thus, depending on the number of violations, the sanctions applied by the CCPA can exceed the amounts registered in the GDPR. Under the LGPD, simple fines of up to 2% of turnover are usually applied, limited to 50 million reals [Lorenzon, 2021].

In summary, GDPR is the law with the greatest scope and coverage of personal data protection among the laws analyzed — followed by LGPD —, as it has a high level of legal maturity compared to the others [Lorenzon, 2021]. Although the ADPPA is the most recent, the economic focus sometimes overrides the right to privacy (as does the CCPA), and the Australian Privacy Act (the oldest), in turn, has a less comprehensive scope compared to current laws [Matulytė, 2022], [Anwar *et al.*, 2018].

Table 3. Comparisons between data privacy laws.

Theme	LGPD	GDPR	ADPPA	Privacy Act	CCPA
Personal Scope	Opt-in consent; Focus on data protection; Children cannot consent	Opt-in consent; Focus on data protection (wide scope); Children cannot consent	Opt-out consent; Focus on corporate freedom; Children can consent from the age of 13	Opt-in consent; Focus on data protection (lower scope); No minimum age for consent	Opt-out consent; Focus on corporate freedom; Children can consent from the age of 13
Territorial Scope	Applies to organizations in or outside Brazil, as long as they process Brazilian data	Applies to organizations in or outside the EU, as long as they process European data	Applies only to the processing of data of individuals residing in the United States	Applies to APP entities (organizations) that may or may not be in Australia	Applies to any for-profit entity doing business in California
Material Scope	Sensitive personal data (direct association); Comprises employee personal data	Sensitive personal data (direct and indirect association); Comprises employee personal data	Sensitive personal data; Does not comprise employee personal data	Sensitive personal data; Comprises employee personal data; Comprises opinion as personal data	Sensitive personal data; Does not comprise employee personal data
Responsible for Treatment	Controller, operator and officer	Controller, processor and DPO	Covered entities and service providers	APP entities	Businesses and service providers
Personal Data	Information relating to an identified or identifiable natural person	Information relating to an identified or identifiable natural person	Covered Data	Any information about an individual held by a federal agency	Information that identifies, describes, or can be associated with a consumer or their family
Sensitive Data	Any information relating to an identified or identifiable person	Any information relating to an identified or identifiable person	Sensitive Covered Data (special categories of personal data)	Any information about an individual held by a federal agency	Information that identifies, describes or can be associated with a consumer or his or her family
Data Processor	Operator (entity that processes personal data on behalf of the controller)	Processor (natural or legal person that performs data processing on behalf of the controller)	Service Provider (service provider that processes data for a covered entity)	Not applicable (focus is on federal agencies as controllers)	Service Provider (entity that processes personal information on behalf of a business)
Penalties	Up to 2% of turnover excluding taxes (limited to 50 million BRL) or daily fine according to total limit	Up to 20 million euros or 4% of total turnover for the previous fiscal year for more serious violations, reduced to up to 10 million euros or 2% of turnover for minor violations	No specifically defined administrative fines, but organizations that violate the ADPPA may still be subject to government enforcement actions and private rights of action	For serious and repeated interference up to $2.500,000 for individuals and up to $50,000,000 for legal entities, or three times the benefit obtained, or 30% of adjusted revenues	From $2,500 to $7,500 dollars per violation and statutory damages between 100 and 750 dollars, offering a 30-day period for correction

4.2 RQ.2: What are the challenges and techniques faced by organizations and developers when adapting to data protection laws in Brazil, the European Union, the USA, and Australia?

Several challenges were identified, ranging from the domain of organizations to developers, to achieve compliance with multiple laws. Canedo *et al.* [2022] and Machado *et al.* [2023] elucidate most of the classes of challenges to be highlighted, referring to LGPD and GDPR, respectively. Of all the selected studies, 168 isolated challenges were identified, and once categorized into classes based on the similarity of these challenges, 18 classes were obtained, in which references can be verified in Zenodo [Rocha and Canedo, 2024]. The categories of challenges, ordered by the quantity identified in the SLR, are shown in **Table 5**. Note that for the challenges identified in the SLR, the identifiers QD (Queried from Documents) were used, covering challenges QD1 to QD18.

QD1. Lack of knowledge of the law: This was the main challenge identified in the SLR, involving both a lack of awareness of the need to implement privacy in software and limited knowledge of existing legislation Sirur *et al.* [2018], [Canedo *et al.*, 2022]. Peixoto *et al.* [2020] reported that, although developers have empirical knowledge about privacy, the biggest obstacle is knowing how to interpret privacy requirements since most of them have no formal knowledge about privacy and LGPD. Thus, the practices that organizations have adopted to solve this challenge are through training and mentoring for developers, as well as the application of seminars [Tahaei *et al.*, 2021], [Sirur *et al.*, 2018].

Table 4. Challenges faced by organizations and developers in the process of complying with data privacy legislation.

ID	Challenge	Qty.
QD1	Lack of knowledge of the law	21
QD2	Translating the law into a technical context	16
QD3	Budget constraints	14
QD4	Lack of team with expertise	14
QD5	Organizational structure	14
QD6	Ambiguity of the law	13
QD7	Lack of standardization of techniques/tools	11
QD8	Lack of security/privacy policy	10
QD9	User relationship	9
QD10	Prioritization of functional requirements	8
QD11	Uncertainty of organizational processes	8
QD12	Difficulties with third-party services	7
QD13	Shortage of guides/tools	5
QD14	International data processing	5
QD15	Changes in development stages	4
QD16	Ethical vs. economic trade-off	4
QD17	Identification of privacy requirements	4
QD18	Impact on application usability	1

QD2. Translating the law into a technical context: A major problem pointed out by developers from different regions is the reading of expressly theoretical standards, in which there is no specification of techniques to achieve compliance [Tahaei *et al.*, 2021], [Davier *et al.*, 2023]. In other words, this complexity makes translating legal requirements into organizational practices difficult, resulting in many de-

velopers being uncomfortable [Tahaei *et al.*, 2021]. To compensate for the lack of specification of techniques in the laws, the adoption of more specific frameworks is a common solution for developers [Machado *et al.*, 2023]), since it allows the standards of current legislation to be combined with the chosen framework [Kühtreiber *et al.*, 2022].

QD3. Budget constraints: It is a common barrier that mainly affects organizations, and developers have little to no influence over it [Teixeira *et al.*, 2019]. This is due to the fact that the process of complying with the law is costly and time-consuming [Teixeira *et al.*, 2019], as it requires recurring financial and human resources, although organizations have them to a limited extent [Rocha *et al.*, 2023]. For small and medium-sized businesses, this challenge is even more critical [Freitas and Mira da Silva, 2018], and a solution proposed by Brodin [2019] would be to use a proactive privacy design, which reveals the contrast with the solution devised by Ayala-Rivera and Pasquale [2018], where solution requirements link GDPR standards and business requirements.

QD4. Lack of team with expertise: It differs from the challenge of a lack of knowledge of the law for the following reason: in this context, companies need additional administrative staff, that is, in most cases, the DPO [Ferrão *et al.*, 2021]. Lack of a team with expertise in current legislation can lead to ineffective risk assessment in data protection [Pires *et al.*, 2021], so a relevant solution is the appointment of a DPO within the organization itself [Ferrão *et al.*, 2021], and in the case of GDPR, the adoption of a controller even allows for the restriction of data flow in the system [Kühtreiber *et al.*, 2022].

QD5. Organizational structure: There is often a communication gap between privacy experts and software developers [Horstmann *et al.*, 2024], which inhibits the proper implementation of privacy in applications due to the absence of the necessary codes of conduct. In addition, organizations can impose limitations on employees, resulting in noncompliance with regulations [Canedo *et al.*, 2022]. In this way, effective knowledge management is fundamental for internal organization and compliance with laws [Davier *et al.*, 2023].

QD6. Ambiguity of the law: Developers face great difficulties in complying with regulations when they are vague, as this makes the process of extracting and implementing these legal requirements complex [Aljeraisy *et al.*, 2022b]. Furthermore, since the requirements are not addressed in a simple and specific language, they are open to various interpretations, which can guarantee a certain level of privacy but not always the one desired by the law [Daoudagh and Marchetti, 2022]. Aljeraisy *et al.* [2022b] also propose solutions, such as a mapping between privacy law and privacy by design schemes, as well as the use of design standards combined with legal guidelines.

QD7. Lack of standardization of techniques/tools: Tahaei *et al.* [2021] highlight the lack of standardization and evaluation metrics since the conceptualization of privacy is volatile, that is, although there are taxonomies and frameworks that conceptualize how privacy should be implemented, there is no consensus among all of them. To add to the complexity, studies show that the decision on privacy also depends on each project [Peixoto *et al.*, 2020], so possible solutions tend to be limited, such as following the guidelines of the application's publishing platform [Ekambaranathan *et al.*, 2021].

QD8. Lack of security/privacy policy: Establishing a consent form and a security policy is a challenge that organizations still neglect today [Canedo *et al.*, 2022]. Freitas and Mira da Silva [2018] pointed out that most of the companies involved did not have a record of security measures, and the challenge may even come from the developers themselves since when using third-party libraries, they do not have a complete understanding of their applications and makes it impossible to properly design a privacy policy [Alomar and Egelman, 2022]. However, it is possible to solve the problem by drafting transparent terms of use, as well as reviewing the legal bases so that an effective and up-to-date security policy can be created [Rocha *et al.*, 2023], in addition to techniques such as Third-Party Tracking and API Configurations [Ekambaranathan *et al.*, 2023].

QD9. User relationship: The difficulty in the relationship between the user and the organization or part of the developers was identified as a challenge in the studies, even in the consent process, since there is a portion of users who are indifferent to the benefits of privacy [Rocha *et al.*, 2023], [Tahaei *et al.*, 2021]. In addition, developers find it very complex to implement transparency — through privacy policies and request systems — in software, further highlighting the challenge [Wiefling *et al.*, 2022]. However, Wiefling *et al.* [2022] showed that renowned companies such as Microsoft and Google already mitigate this problem through self-service tools or, similarly, privacy dashboards.

QD10. Prioritization of functional requirements: With regard to the prioritization of functional requirements by developers, studies pointed to a number of factors to be taken into account, such as reduced system performance, tight deadlines for implementing effective security, or simply the difficulty in implementing non-functional requirements [Machado *et al.*, 2023], [Li *et al.*, 2020], [Rocha *et al.*, 2023]. So, there is an identified tension between priorities and the prioritization of functional requirements to the detriment of security and privacy [Tahaei *et al.*, 2021]. As a solution, the application of automated tests can favor the importance given to non-functional requirements, and the use of methods that contribute to the rapid updating of applications and effective feedback can also motivate developers to improve both categories of requirements [Li *et al.*, 2022].

QD11. Uncertainty of organizational processes: Developers may not always be familiar with all organizational processes, complicating compliance with data protection legislation. This leads to challenges in data backup adequacy, auditing systems, and using cloud services, which depend on the physical location of data storage [Machado *et al.*, 2023], [Poritskiy *et al.*, 2019], [Nurgalieva *et al.*, 2023]. Based on this, a good starting point for mitigating the risks of uncertainty is through access logs when it comes to data processing and opting for cloud providers that are compatible and guarantee compliance with current legislation [Machado *et al.*, 2023].

QD12. Difficulties with third-party services: Alomar and Egelman [2022] shows that a large part of privacy problems stems from the use of third-party Software Development Kits (SDKs). As such, one of the main challenges pointed out by developers is navigating the privacy implications of these libraries. Likewise, it is unclear how the libraries will process personal data [Ekambaranathan *et al.*, 2023], [Ekambaranathan *et al.*, 2021]. To address this challenge, solutions include prioritizing libraries from prominent providers and, whenever possible, avoiding sharing data that is not absolutely necessary with third-party services [Ekambaranathan *et al.*, 2021].

QD13. Shortage of guides/tools: The lack of specific guides for applying privacy in a software context is a problem highlighted both by Brazilian and European developers [Alhazmi and Arachchilage, 2021], [Rocha *et al.*, 2023]. Ekambaranathan *et al.* [2021] identified, through interviews, that many application developers had difficulty finding adequate and specific design guidelines and that when they did, there was insufficient support for smaller companies. Thus, solutions such as focusing on a good user experience and consulting professionals without guides and tools were elucidated in the work [Ekambaranathan *et al.*, 2021].

QD14. International data processing: When it comes to organizations that process people's data globally, there is a major challenge regarding which legislation to prioritize [Sirur *et al.*, 2018]. As discussed in RQ.1, laws have many points of divergence, which can lead to expectations of judicial response and contractual difficulties [Sirur *et al.*, 2018], [Freitas and Mira da Silva, 2018]. Furthermore, all other challenges are summed up in this one since a common solution must be found to the difficulties of ensuring compliance with multiple laws. On a practical level, a good starting point is to map and analyze the data flow [Sirur *et al.*, 2018], and the use of tools and automation can facilitate the technical compliance process.

QD15. Changes in development stages: In the process of developing a product, changes are common at some stage, ranging from infrastructure and data growth to system readjustments to make them more compatible in a certain aspect [Canedo *et al.*, 2022], [Li *et al.*, 2020]. Although these changes are sometimes necessary, it is a fact that they increase technical complexity and require reformulations in techniques that implement privacy in software [Li *et al.*, 2020]. Li *et al.* [2022] explained the challenge of balancing GDPR compliance in a competitive data business environment and, based on this, a solution pointed out in the study is the use of continuous software engineering since it unites rapid updates and feedback, and enables the accelerated correction of points of non-compliance.

QD16. Ethical vs. economic trade-off: Organizations often face the challenge of balancing respect for privacy with prioritizing corporate freedom [Neves, 2021]. Since a company's primary objective is economical, given the nature of the business [Li *et al.*, 2020], the focus on privacy and protection of personal data can be placed on a low-priority agenda [Pitogo and Ching, 2018], leading to cutting corners in security. Rocha *et al.* [2023] showed that organizations must consider, on an economic level, the possible penalties in the event of non-compliance with legislation and that reduced reliability on the part of customers causes a competitive disadvantage in the long term, which could lead to financial losses for the organization.

QD17. Identification of privacy requirements: As discussed above, developers generally have empirical knowledge about privacy, but identifying an application's privacy requirements, in light of data protection legislation, is considered a complex task [Peixoto *et al.*, 2020]. Therefore, it is necessary to use a device to help comply with the law in force, such as the User Stories specification, to facilitate the requirements analysis stage [Canedo *et al.*, 2022]. Furthermore, as a technique used in agile teams, a possible solution would be to use Design Thinking tools in the requirements elicitation stage [Canedo *et al.*, 2021a].

QD18. Impact on application usability: This is mainly a problem for small and medium companies as if data processing power is not sufficient, the addition of a privacy and data protection framework could reduce the performance of the system or make it impossible to use an application [Brodin, 2019]. It is recommended to use specific frameworks as early as possible, that is, in the application design process [Brodin, 2019], to estimate and avoid performance risks.

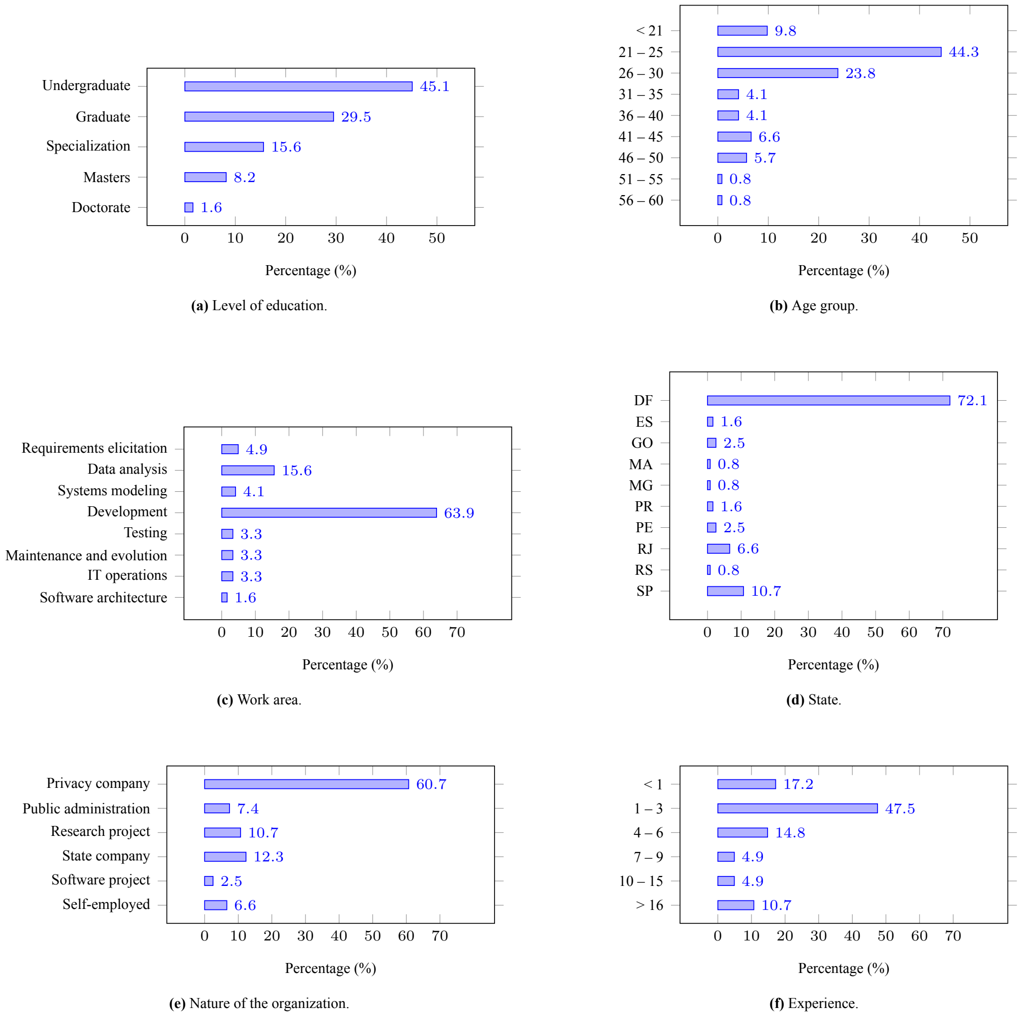
In summary, the main challenges for ensuring compliance are related to the process of understanding the law. A massive number of developers and organizations still have difficulty understanding the theory of the law and how to apply it in a technical context. Restrictions imposed by organizations and a lack of suitable material to help developers implement privacy in software have also been identified as major challenges.

4.3 Survey

To perform an initial mapping, the participants were grouped by education level (Q3) and age (Q1): most of the respondents were undergraduate students (45,1%); however, in a broader view, 54,9% had an undergraduate or postgraduate degree (see **Figure 4a**); and a good portion of the participants (44,3%) are between the ages of 21–25 and, considering a small increase in the range, almost 70% are between 21–30 years of age (see **Figure 4b**).

Concerning the stages of software development in which the participants worked (Q4), in addition to the six initially defined, there is an answer when the respondent inserted any area that was not present among the survey alternatives. Hence, it was essential to define two categories and their areas: IT Operations, which encompasses infrastructure, production, consulting, and management; and Software Architecture, focusing on the architecture in itself as well as system engineering. So, most of the participants (63,9%) work in the area of software development (see **Figure 4c**).

Regarding the location (Q2) and the origin of the organization (Q5), almost three quarters (72,1%) of the respondents live in the Federal District (see **Figure 4d**) and the majority (60,7%) are employed by a private company (see **Figure 4e**). Regarding professional experience in their current job (Q6), almost half (47,5%) have 1 to 3 years of experience, and only 35,3% have more than 3 years of experience (see **Figure 4f**). This information, together with the level of education and age group, confirms the hypothesis that a significant proportion of participants have only recently entered the professional world.



(a) Level of education.

(b) Age group.

(c) Work area.

(d) State.

(e) Nature of the organization.

(f) Experience.

Figure 4. Participants' profile: demographic data.

The respondents were also asked to express their opinions about their familiarity with LGPD (Q7) in order to help structure the profile of the participants. Thus, 80% of the participants agreed that they were already familiar with or knew about LGPD, and only 3% definitely did not. Furthermore, to analyze open-ended answers (Q9 to Q12), the evolved Grounded Theory process was adopted [Chun Tie *et al.*, 2019], which is applied based on the following steps and their respective descriptions:

1. Data collection: Based on the SLR, with the main challenges of implementing data protection laws already identified, the proposed survey aimed to validate and identify new challenges and techniques. Thus, the data collection did not initially present pre-defined hypotheses since the aim is to explore the challenges and techniques in an open way in order to discover new patterns.

2. Open Coding: A line-by-line analysis of the answers was carried out using spreadsheet structuring, with the aim of segmenting and categorizing them, i.e., relating them to the patterns identified in the SLR. There would be a new category for the challenge if there were no such patterns.

3. Axial coding: Once the categories had been drawn up, most of which had already been defined in the SLR, an analysis was made of how the techniques explained by the respondents matched the challenges presented, with the aim of quantifying and classifying them. To this end, the best techniques and ways to mitigate the challenges (Q10 and Q11) were taken as a reference to solve each respondent's respective challenges (Q9).

4. Selective Coding: A more focused analysis was carried out on the central categories that emerged from the previous phases. Based on these categories, an attempt was made to understand how mitigation techniques were connected to the most recurrent challenges, aiming to refine and select the most relevant categories, for example, difficulties in understanding the law and translating it into a technical context. The focus was then on synthesizing the information and identifying key patterns to build the final theory.

5. Grounded Theory: Based on the categories already refined, it was possible to develop a grounded theory that explains the challenges faced by developers in implementing the LGPD, including the new challenges identified. This theory was built from the collected data to reflect the relationships between the challenges and the solutions proposed by the participants and explain the emerging patterns that emerged in the study.

4.4 Challenges and Techniques

The results of the challenges are shown in **Figure 5** (reorganized after the survey results), and it is important to note that the participants suggested three challenges that had not yet been elucidated by the SLR. These new challenges feature QN (Queried from Narratives) identifiers and cover the following challenges: a development process not evaluated as required by the LGPD (QN1); projects created without privacy by default (QN2); and constant changes to the law (QN3). In addition, the proposed guide has mapped and documented information on the challenges already identified in the SLR and possible solutions and mitigation techniques.

It should be noted that most of the challenges classified in the SLR maintained their position even after the survey was applied, such as QD1, which was considered the biggest challenge in both the SLR and the survey. In general, challenges related to legislation and developers were considered more important in the survey than in the SLR, while there was less focus on challenges originating from organizations themselves. **Table 5** shows a brief correlation between the challenges and potential solutions. Also, the complete set of techniques and specifications, as well as the transcriptions of the participants' can be found on Zenodo [Rocha and Canedo, 2024].

5 Framework Analysis

As discussed in the methodology, the Framework Analysis method was adopted to fill the gaps identified in the SLR. For the current work, the five stages are as follows [Goldsmith, 2021]:

1. Data Familiarization: Initially, the five privacy laws were read in full, so the comparison with PbD and ISO/IEC 29100 was added to the guide later. This process is particularly important for understanding the terms used in each excerpt of the laws.

2. Framework Identification: After reading the laws in full, it is necessary to identify the relevant themes that are present in all the legislation. Since the themes had already been identified in the SLR, they were simply organized into separate tables to facilitate subsequent graphic visualization. The whole process was recorded in a spreadsheet (Google Sheets), as this is a relatively time-consuming method (as it requires reading all the legislation in full), and it is necessary to have quick and easy access to each stage. Therefore, the key themes identified were: scope (with personal, territorial, and material sub-themes); definitions (with personal data, sensitive data, responsible for treatment, and data processor sub-themes); penalties; principles; and individual rights.

3. Indexing: Next, the indexing process was only necessary in the absence of information identified in the SLR, i.e., for the topics of principles, penalties and additionally for individual rights, since not all laws have the same rights. Thus, for these themes, we identified their particularities in the laws and ordered them based on a general theme. Since the process involves questions about how similar or different an excerpt of a legislation is to another, categories of similarity were also drawn up so that:

   - ✓ - Y/S: Present and identified in the literature review;
   - ✓ - Y/O: Present and identified directly in the law (in the same section);
   - ✓ - Y/D: Present in another section of the law, but similar;
   - ✓ - Y/C: Present, but applied to a different context (requires specification for application);
   - ✕ - N/A: Not found in the articles or in the law.

   The categories were essential for the next stage of the framework analysis since the LGPD was adopted as the basis for the comparative process of principles and rights. Thus, for the other laws, the equivalent principles and rights were adapted (in addition to their level of equivalence, according to the categories).

4. Charting: The identified themes were graphically mapped, and their definitions were generalized. Although the particularities of each piece of legislation were not eliminated, the generalization helped to categorize the similarities and differences more clearly without reducing the complexity of the themes.

5. Mapping and Interpretation: For complex topics, such as principles and definitions, a detailed mapping was made using similarity categories and including explanatory comments in the spreadsheet. In addition, three researchers reviewed the process to ensure that the interpretations and classifications were correct and consistent.

Before applying the appropriate categories, the researchers determined whether each theme was present in the legislation. For instance, a principle was classified as ”Y/S” if found in the SLR or ”Y/O” if mentioned explicitly in the law in the principles section. Moreover, it was classified as ”Y/D” if it appeared in a different part of the law but had comparable wording and meaning (for instance, the purpose principle is considered a right in the CCPA). Also, it was classified as ”Y/C” when applied to a different setting or jurisdiction, that is, if a specific setting is required (for example, the open access principle only applies to large data holders when it comes to ADPPA).

Also, we conducted an iterative review procedure to guarantee accuracy and consistency in the classification. Following the first categorization, three researchers examined the categories independently to find any inconsistencies or unclear areas in the laws' interpretation, focusing on the syntactic analysis of the laws. When disagreements emerged, the researchers deliberated and came to an agreement based on the relevant legal text and principles. It is expected that this cooperative process made accurate and uniform interpretations and classifications across all laws possible.

Furthermore, **Table 6** shows a comparison of the principles and rights of each legislation and the appropriate coverage of the frameworks. In the guide, it is possible to check

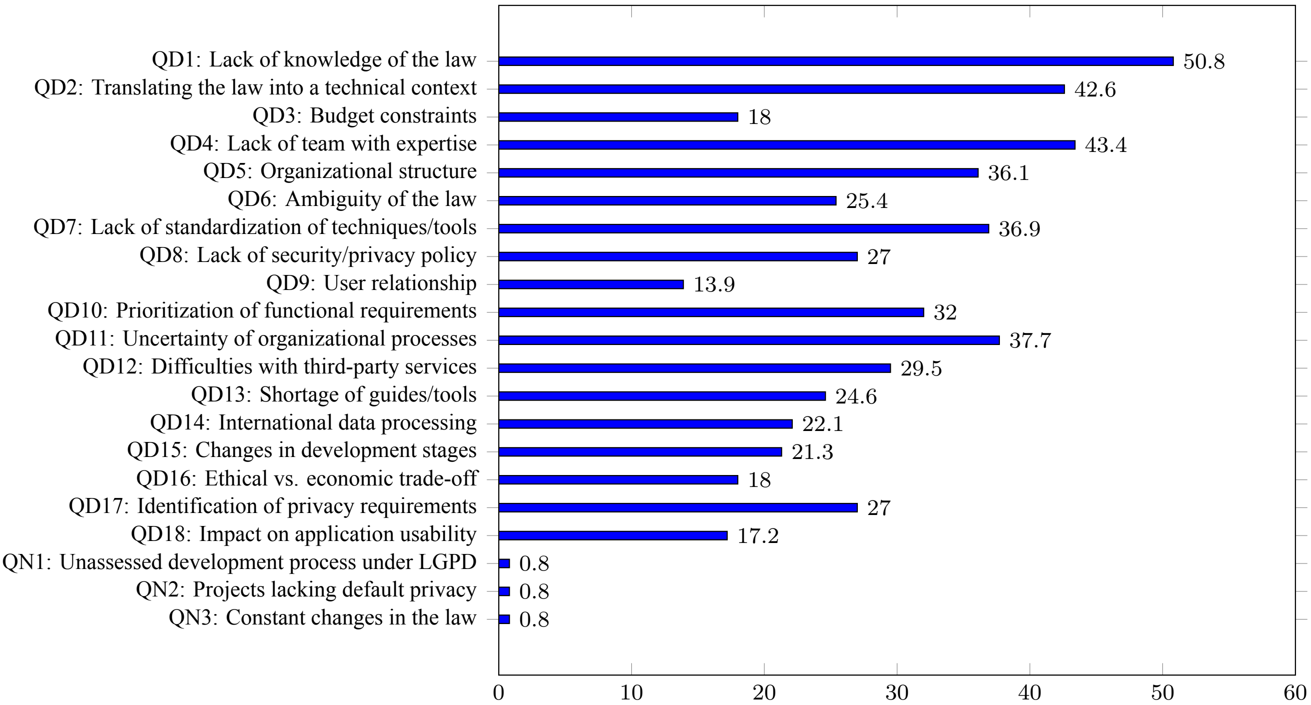


Figure 5. Challenges presented by the participants (%).

Table 5. Challenges in privacy compliance and potential approaches.

Challenge	Potential Approaches
Lack of knowledge of the law	Establishing internal governance guidelines, supporting specialized training programs, and putting in place ongoing instruction on data handling and legal requirements.
Lack of team with expertise	Employing legal counsel, hiring Data Protection Officers (DPOs), and utilizing AI technologies to automatically identify sensitive information.
Translating the law into a technical context	Adopting open-source tools for compliance, implementing the organizational Information Classification Policy, and putting into practice information classification policies that emphasize privacy-oriented design frameworks.
Uncertainty of organizational processes	Implementing access logs and data minimization techniques, enforcing clear documentation, and establishing robust data governance.
Lack of standardization of techniques/tools	Utilizing Agile approaches, abiding by platform policies that facilitate encryption, anonymization, and access control, and respecting established privacy frameworks.
Organizational structure	Adopting restricted data access policies, implementing strategic communication programs, and implementing security measures such as row-level security (RLS).
Prioritization of functional requirements	Implementing automated privacy testing, incorporating privacy into Agile processes, and promoting Privacy by Design principles, while continuously mapping personal data.
Difficulties with third-party services	Keeping an updated list of dependencies, verifying third-party vendors, and enforcing compliance provisions in contracts.
Lack of security/privacy policy	Creating clear privacy policies, ensuring that data is anonymized and encrypted, and implementing stringent access control measures.
Identification of privacy requirements	Working with compliance teams, applying Design Thinking techniques, and adopting user story specifications.
Ambiguity of the law	Mapping legal requirements to privacy frameworks, practicing data minimization, and using encryption techniques, in order to minimize damage regarding data breaches.
Shortage of guides/tools	Creating developer-friendly privacy documentation, collaborating with experts, and developing open-source privacy tools.
International data processing	Establishing transparent governance guidelines, making sure that international privacy laws are taught, and adhering to international data transfer protocols.
Changes in development stages	Incorporating compliance checks into CI/CD pipelines, implementing ongoing privacy impact assessments, and consulting legal experts on significant updates.
Budget constraints	Employing open-source privacy tools, giving proactive privacy design top priority, and striking a balance between economical privacy tactics.
Ethical vs. economic trade-off	Establishing strict legal sanctions, guaranteeing openness in data usage, and encouraging business models that respect privacy.
Impact on application usability	Utilizing effective encryption algorithms, optimizing privacy-preserving methods, and incorporating privacy measures early in the development process.
User relationship	Supplying privacy dashboards and self-service tools, as well as incorporating users in the consent and data processing procedures.
Unassessed development process under the LGPD	Establishing guidelines to map requirements and utilizing established frameworks to guarantee LGPD compliance from the outset.
Projects lacking default privacy	Incorporating privacy from the beginning of development, employing the Privacy by Design framework, and setting restrictive privacy defaults.
Constant changes in the law	Maintaining up-to-date project documentation, updating software, and creating an efficient incident response plan (IRP).

how these guidelines relate to each other, providing a complete developer experience. It is possible to check both processes step by step in Zenodo [Rocha and Canedo, 2024] and complement the discussion and presentation of the techniques in the proposed guide.

As a basis, the ten principles established by the LGPD in

Table 6. Comparisons between data privacy laws.

Principles/Rights	LGPD	GDPR	ADPPA	Privacy Act	CCPA	PbD	ISO/IEC 29100
Purpose	✓ Y/S	✓ Y/S	✓ Y/D	✓ Y/S	✓ Y/S	×	✓
Adequacy	✓ Y/S	✓ Y/S	✓ Y/D	✓ Y/S	✓ Y/S	✓	✓
Needs	✓ Y/S	✓ Y/S	✓ Y/D	✓ Y/S	✓ Y/S	✓	✓
Open Access	✓ Y/S	✓ Y/D	✓ Y/C	✓ Y/S	✓ Y/D	✓	✓
Data Quality	✓ Y/S	✓ Y/S	✓ Y/D	✓ Y/S	× N/A	✓	✓
Transparency	✓ Y/S	✓ Y/S	✓ Y/D	✓ Y/S	✓ Y/S	✓	✓
Security	✓ Y/S	✓ Y/S	✓ Y/D	✓ Y/S	✓ Y/S	✓	✓
Prevention	✓ Y/S	✓ Y/D	✓ Y/D	✓ Y/O	× N/A	✓	✓
Non-discrimination	✓ Y/S	✓ Y/D	✓ Y/D	× N/A	✓ Y/S	✓	×
Accountability	✓ Y/S	✓ Y/S	✓ Y/C	× N/A	✓ Y/S	×	✓
Minimized Collection	✓ Y/S	✓ Y/D	✓ Y/S	✓ Y/D	✓ Y/C	✓	✓
Confirmation of Existence of Treatment	✓ Y/S	✓ Y/S	× N/A	✓ Y/D	✓ Y/S	✓	✓
Data Access	✓ Y/S	✓ Y/S	✓ Y/O	✓ Y/D	✓ Y/S	✓	✓
Data Correction	✓ Y/S	✓ Y/S	✓ Y/O	✓ Y/S	✓ Y/O	×	✓
Anonymization	✓ Y/S	✓ Y/C	× N/A	✓ Y/D	× N/A	×	✓
Data Portability	✓ Y/S	✓ Y/S	✓ Y/S	× N/A	✓ Y/S	✓	✓
Data Deletion	✓ Y/S	✓ Y/S	✓ Y/O	× N/A	✓ Y/S	×	✓
Information on Participating Entities	✓ Y/S	✓ Y/O	✓ Y/O	✓ Y/D	✓ Y/O	✓	✓
Information on the Possibility of Not Consenting	✓ Y/S	✓ Y/D	✓ Y/C	× N/A	✓ Y/O	✓	✓
Revocation of Consent	✓ Y/S	✓ Y/D	✓ Y/O	✓ Y/S	✓ Y/S	✓	✓
Dispute	✓ Y/O	✓ Y/S	✓ Y/O	× N/A	✓ Y/S	✓	✓
Purpose Consistent Processing	✓ Y/D	✓ Y/D	✓ Y/S	✓ Y/D	✓ Y/O	✓	✓
Retention Consistent with Purpose	✓ Y/D	✓ Y/D	✓ Y/S	✓ Y/D	× N/A	✓	✓
Opposition to Automated Decision Making	✓ Y/O	✓ Y/S	× N/A	× N/A	× N/A	✓	×
Processing Restriction	✓ Y/C	✓ Y/S	× N/A	× N/A	✓ Y/O	✓	×

Art. 6° [Brasil, 2018] and the individual rights explained by both the LGPD and the GDPR, discussed in Chapter 3 in both laws [Brasil, 2018], [European Parliament and Council, 2018], in order to massify this topic. The equivalence between the principles has a theoretical basis when identified in the articles (Y/S), such as the relationship between the Purpose principle (LGPD) and the Purpose Limitation (GDPR) [Canedo *et al.*, 2020].

Thus, for principles that do not have a direct equivalence, it was necessary, through framework analysis, to index and map them, even if there was variation in the terminology used in each piece of legislation. It is worth noting that since there is no specific section for the principles in the ADPPA or the CCPA, there is no occurrence of the Y/O category, i.e., a case where there is a principle in the law and it is presented in the same section, that is, the principles section.

The GDPR presents most of the principles equivalent to the LGPD, as stated in **Table 6**, but three have been identified in another section of the law, acting similarly to the LGPD. The principles of Open Access, Prevention, and Non-discrimination are considered individual rights by the GDPR and are equivalent respectively to: Right of access by the data subject — Art. 15 —, for Open Access; and Restrictions — Art. 23 —, for Prevention and Non-discrimination [European Parliament and Council, 2018].

ADPPA was the most difficult to identify in the SLR, and, in addition, since it does not have a section on principles, the equivalence analysis is even more complex. Most of the principles were associated with Data Minimization — SEC. 101 [U.S. Congress and Commerce, 2022] —, such as Purpose, Adequacy, Needs, Prevention, and Non-discrimination. In addition, there are principles that correlate with individual rights under the law, such as Data Quality, Transparency, and Security, which are, respectively, elucidated in the ADPPA through the Right of Correction – SEC. 203, Right of Transparency – SEC. 202 and Right of Data Security – SEC. 208 [U.S. Congress and Commerce, 2022].

Also, the ADPPA correlates with two principles of the LGPD that are only applicable in specific situations, i.e., for large data holders. The principles of Open Access and Accountability are identified in the SEC. 301 [U.S. Congress and Commerce, 2022] and only deal with privacy impact assessments for large data holders, i.e., they are less comprehensive when compared to LGPD and GDPR.

Australian privacy law, similar to the GDPR, has a large number of principles that were identified in the SLR as equivalent. The principle of Prevention is guaranteed as a consequence of the principle of Security, i.e., it is given as equivalent to APP 11 – security of personal information [OAIC, 1988]. However, principles such as Non-discrimination and Accountability were not identified, neither in the SLR nor in the framework analysis process.

Finally, the CCPA also presents numerous principles equivalent to the LGPD and GDPR, although Open Access is presented in the legislation as an individual right through Section 1798.110. Consumers' Right to Know What Personal Information is Being Collected. Right to Access Personal Information [State of California, 2018]. The Data Quality principle is pointed out, through the SLR, as not existing in the CCPA [Aljeraisy *et al.*, 2022b], while the Prevention principle was not identified by the framework analysis.

Regarding individual rights, it is interesting to note that in Australian law, the oldest among those studied, there is no exclusive section for individual rights, so they are identified in different sections of the law. In addition, for the other laws, there are rights that are considered principles (and vice versa) or even in exceptional sections, such as the ADPPA's Duty of Loyalty. It is worth recalling that, as the individual rights framework was created on the basis of the LGPD and GDPR, both pieces of legislation include most of the rights already identified in the SLR.

With regard to the rights not identified in the LGPD's SLR, those of Dispute and Opposition to Automated Decision Making are identified in the rights section itself, respectively, in Art. 18° — §1 and §2 — and Art. 20° [Brasil, 2018]. The rights to Purpose Consistent Processing and Retention Consistent with Purpose can be understood in a single principle, already established in the LGPD, since it guarantees that processing will be carried out only for legitimate purposes and without the possibility of further processing in a manner incompatible with those purposes [Brasil, 2018]. The right to Processing Restriction is covered by the LGPD in Art. 15°, but there are specific situations in which the restriction can occur (it is less comprehensive than the GDPR).

The GDPR, unlike the LGPD, presents a series of rights that are already included in the principles section, such as: Minimized Collection (Art. 5 – Data Minimization), Information on the Possibility of Not Consenting (Art. 7 – Conditions for consent), Revocation of Consent (Art. 7 – Conditions for consent), Purpose Consistent Processing (Art. 5 – Storage limitation) and Retention Consistent with Purpose (Art. 5 – Storage limitation) [European Parliament and Council, 2018]. In addition, the GDPR treats the anonymization process as pseudonymization, as addressed in Art. 4 [European Parliament and Council, 2018]. Finally, the right of Information on Participating Entities is found in the same section, through Art. 13 (Information to be provided where personal data are collected from the data subject) [European Parliament and Council, 2018].

With regard to the ADPPA, few rights have been identified in the SLR, but the legislation presents a range of rights, which can be seen in the rights section itself. The prerogatives of Data Access, Correction, and Deletion are all guaranteed through the SEC. 203 – Individual data ownership and control, while the right to Information of Participating Entities is guaranteed by SEC. 202 – Transparency and the rights of Revocation of Consent and Dispute are included in the SEC. 204 – Right to consent and object [U.S. Congress and Commerce, 2022].

The right to be informed of the possibility of not consenting is also present in the ADPPA, but there are restrictions. The same is included in the SEC. 202 – Transparency, but it is applicable in case of a change in the terms of consent [U.S. Congress and Commerce, 2022]. As such, its scope is more limited than that of the LGPD and GDPR. Compared to the other laws, on the other hand, ADPPA presents four rights that were not identified through the framework analysis, as shown in **Table 6**: Confirmation of Existence of Treatment, Anonymization, Opposition to Automated Decision Making, and Processing Restriction.

Under Australian law, some rights are guaranteed through principles since there is no explicit section for individual rights. The correlation between them is given by: Minimized Collection (APP 3 – collection of requested personal information); Confirmation of Existence of Treatment (APP 12 – access to personal information); Anonymization (APP 2 – anonymity and pseudonymity); Information on Participating Entities (APP 1 – open and transparent management of personal information); Revocation of Consent (APP 3 – collection of requested personal information / APP 6 – use or disclosure of personal information); Purpose Consistent Processing (APP 6 – use or disclosure of personal information); Retention Consistent with Purpose (APP 11 – security of personal information) [OAIC, 1988].

There is also a right that is not related to the principles in Australian law, which is Data Access, referring to Section 20, Subdivision F (Access to, and correction of, information). Half of the unidentified rights have been elucidated in the SLR, which are the rights to Data Portability, Opposition to Automated Decision Making, and Processing Restriction [Aljeraisy *et al.*, 2022b]. The framework analysis process did not identify the other rights (Data Deletion, Information on the Possibility of Not Consenting, and Dispute).

Finally, the CCPA also presents several rights that are found in an explicit rights section. The prerogatives of Data Correction, Information of Participating Entities, Information of the Possibility of Not Consenting, Purpose Consistent Processing, and Processing Restriction are equivalent to the rights of, respectively: Right to Correct Inaccurate Personal Information, Right to Know What Personal Information is Sold or Shared and to Whom, Right to Opt Out of Sale or Sharing of Personal Information, Right to Know What Personal Information is Being Collected. Right to Access Personal Information and Right to Limit Use and Disclosure of Sensitive Personal Information. [State of California, 2018].

Minimized Collection, in turn, is equivalent to the Right to Limit Use and Disclosure of Sensitive Personal Information. Still, it is only adopted if there is a request from the data subject. This reinforces the idea of opt-out consent, highlighted in **Table 3**. The rights of Anonymization and Opposition to Automated Decision Making were identified as non-existent in the CCPA [Aljeraisy *et al.*, 2022b], and through the framework analysis, it was not possible to identify the right of Retention Consistent with Purpose.

6 Proposed Guide

The proposed guide, named 5L2FGuide[2] — 5 Laws, 2 Frameworks Guide — was developed as a web-based resource, freely accessible at 5L2FGuide, with open-source code available on GitHub[3]. It includes navigable pages such as Introduction, Scope, Definitions, Principles, Rights, Challenges, and About. The guide aims to help developers and organizations ensure compliance with privacy laws through Privacy by Design and ISO/IEC 29100 frameworks, informing their coverage of the laws regarding principles and individual rights.

The Introduction page presents the guide's purpose: how developers and their respective organizations can ensure compliance with privacy legislation through the Privacy by Design and ISO/IEC 29100 frameworks. For developers who have little or no knowledge of the laws, an information carousel has been implemented, which introduces each of the laws and frameworks to readers. The About page follows the same structural pattern but provides information about the author and advisor and the references used to prepare the guide.

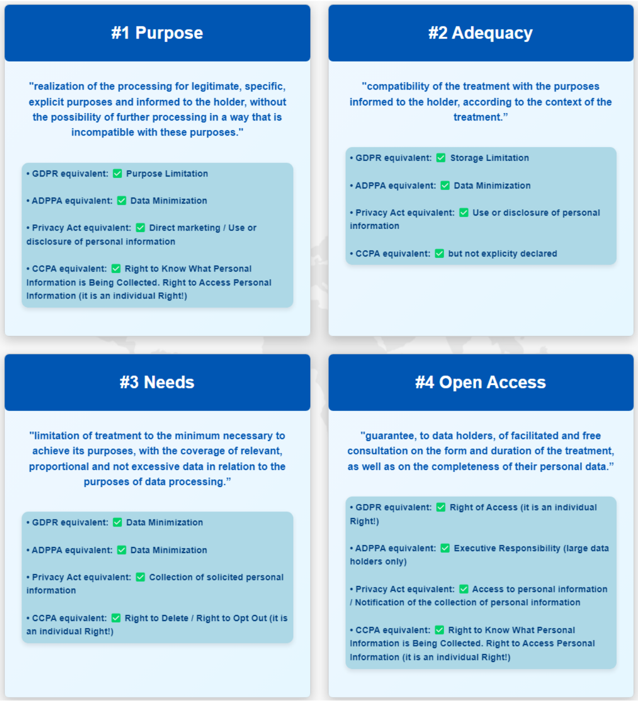
[2] https://xdalle.github.io/5L2FGuide

[3] https://github.com/xDalle/5L2FGuide

The Scope and Definitions pages also share the same structure. They provide a brief explanation of the scope and definitions of the legislation, respectively, and detail the essential terms used in the guidelines. These pages are based solely on the information presented in **Table 3**, which was derived from the SLR results, available at Zenodo [Rocha and Canedo, 2024].

The Challenges page, on the other hand, similarly presents a quick introduction to organizational challenges and their mitigation techniques to ensure compliance with data protection laws. It is also structured according to the challenges identified in the SLR and the new issues discovered by the survey, as shown in **Figure 5**. In addition, mitigation techniques have been added, as shown in Zenodo [Rocha and Canedo, 2024].

The Principles and Rights pages feature an interactive game that allows users to select compliance goals, comparing frameworks and their coverage percentages. The user must choose between the cards required for compliance in their organization (see **Figure 6**), and the percentage of coverage of these principles and rights by each framework is presented (see **Figure 7**), which helps the developer to choose the one that best meets their demands. To facilitate this selection for developers who know only one of the laws or a small set, the reader is presented with the equivalence of principles and rights explored in the Framework Analysis stage. The connection between principles and rights can be seen through the Zenodo [Rocha and Canedo, 2024].



#1 Purpose

"realization of the processing for legitimate, specific, explicit purposes and informed to the holder, without the possibility of further processing in a way that is incompatible with these purposes."

- GDPR equivalent: ✅ Purpose Limitation
- ADPPA equivalent: ✅ Data Minimization
- Privacy Act equivalent: ✅ Direct marketing / Use or disclosure of personal information
- CCPA equivalent: ✅ Right to Know What Personal Information is Being Collected. Right to Access Personal Information (it is an individual Right!)

#2 Adequacy

"compatibility of the treatment with the purposes informed to the holder, according to the context of the treatment."

- GDPR equivalent: ✅ Storage Limitation
- ADPPA equivalent: ✅ Data Minimization
- Privacy Act equivalent: ✅ Use or disclosure of personal information
- CCPA equivalent: ✅ but not explicity declared

#3 Needs

"limitation of treatment to the minimum necessary to achieve its purposes, with the coverage of relevant, proportional and not excessive data in relation to the purposes of data processing."

- GDPR equivalent: ✅ Data Minimization
- ADPPA equivalent: ✅ Data Minimization
- Privacy Act equivalent: ✅ Collection of solicited personal information
- CCPA equivalent: ✅ Right to Delete / Right to Opt Out (it is an individual Right!)

#4 Open Access

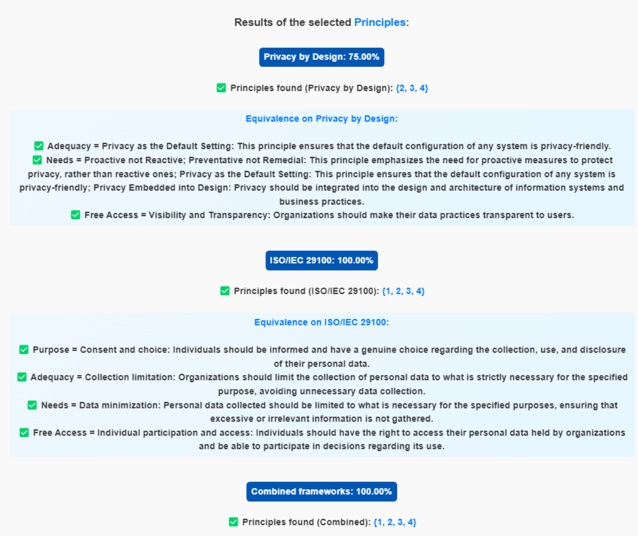
"guarantee, to data holders, of facilitated and free consultation on the form and duration of the treatment, as well as on the completeness of their personal data."

- GDPR equivalent: ✅ Right of Access (it is an individual Right!)
- ADPPA equivalent: ✅ Executive Responsibility (large data holders only)
- Privacy Act equivalent: ✅ Access to personal information / Notification of the collection of personal information
- CCPA equivalent: ✅ Right to Know What Personal Information is Being Collected. Right to Access Personal Information (it is an individual Right!)

Figure 6. Example of cards used in Principles section.

6.1 Guide Validation

The guide validation survey was developed using the Google Forms platform, with an estimated completion time of 15 minutes. The guide was introduced to two postgraduate Privacy and Information Security classes, during the subject of Privacy Management and Personal Data Protection. Participants were asked to explore the guides' sections, from comparative analysis to interactive games, and only then to complete the survey.



Results of the selected Principles:

Privacy by Design: 75.00%

✅ Principles found (Privacy by Design): {2, 3, 4}

Equivalence on Privacy by Design:

✅ Adequacy = Privacy as the Default Setting: This principle ensures that the default configuration of any system is privacy-friendly.
✅ Needs = Proactive not Reactive; Preventative not Remedial: This principle emphasizes the need for proactive measures to protect privacy, rather than reactive ones; Privacy as the Default Setting: This principle ensures that the default configuration of any system is privacy-friendly; Privacy Embedded into Design: Privacy should be integrated into the design and architecture of information systems and business practices.
✅ Free Access = Visibility and Transparency: Organizations should make their data practices transparent to users.

ISO/IEC 29100: 100.00%

✅ Principles found (ISO/IEC 29100): {1, 2, 3, 4}

Equivalence on ISO/IEC 29100:

✅ Purpose = Consent and choice: Individuals should be informed and have a genuine choice regarding the collection, use, and disclosure of their personal data.
✅ Adequacy = Collection limitation: Organizations should limit the collection of personal data to what is strictly necessary for the specified purpose, avoiding unnecessary data collection.
✅ Needs = Data minimization: Personal data collected should be limited to what is necessary for the specified purposes, ensuring that excessive or irrelevant information is not gathered.
✅ Free Access = Individual participation and access: Individuals should have the right to access their personal data held by organizations and be able to participate in decisions regarding its use.

Combined frameworks: 100.00%

✅ Principles found (Combined): {1, 2, 3, 4}

Figure 7. Example of frameworks coverage in Principles section.

Participants were informed that their participation was anonymous, voluntary, and solely for research purposes and that consent was required. It was also explained that the process could be interrupted at any time without penalties, and the author was available for questions during the survey application to ensure smooth interaction with the guide.

The survey consisted of two parts: participants' profiles and guide validation. Questions Q01 to Q05 aimed to identify and sectorize the sample, while Q06 to Q08 explored respondents' theoretical and practical experience of data protection laws. **Table 7** shows the questions designed for this stage of the survey.

Table 7. Survey questions related to participants' profile and experience with data protection laws.

ID	Question
Q01	Which state are you from?
Q02	What is your level of education?
Q03	What is your current role in your job?
Q04	How many years of experience do you have in Data Privacy?
Q05	What is the nature of the organization you work for?
Q06	Have you ever researched or worked with data protection laws?
Q07	Do you currently research or work with data protection laws?
Q08	What is your level of experience or knowledge of data protection laws?

For part two, questions Q09 to Q17 were based on the Technology Acceptance Model (TAM) [Davis, 1989] using a Likert scale, assessing usability (Q09 to Q13) and ease of use (Q14 to Q17). Usability measures how well the guide enhances the user's work, while ease of use quantifies whether the guide requires minimal effort to use.

Finally, open-ended questions (Q18 to Q20) invited participants to express in their own words the guide's strengths (Q18) and weaknesses (Q19), as well as suggestions for improvements (Q20). The latter is intended to improve the guide's content, design, compatibility, and scalability.

The survey collected 37 responses, and both questions and answers (in full and graphically) can be found in Zenodo [Rocha and Canedo, 2024]. Regarding the level of education (Q02), since the questionnaire was applied to postgraduate classes, the undergraduate category was not included. Thus, most respondents had a specialization (45,9%) or a master's degree (29,7%), and, to a greater extent, 86,5% of the participants had a postgraduate degree.

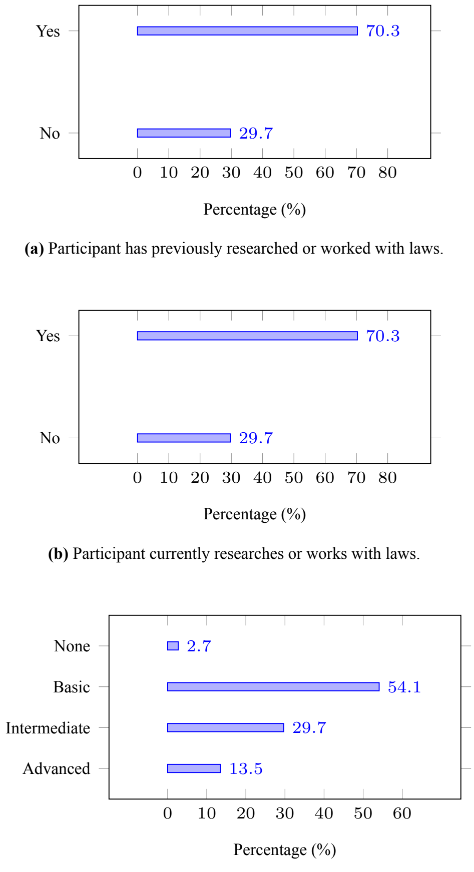
The participants' area of activity (Q03) was shown to be varied and balanced, but most of them were information security analysts (21,6%). There was a significant number of information security managers and data clerks (with 16,2% in each category), as well as project managers, IT management and governance, and IT operations (with 10,8% in each category). There were also professionals working in compliance, internal audit coordination, information analysis, and systems architecture, but to a lesser extent (5,4% for the first and 2,7% for the others).

Regarding the location (Q01) and the nature of the organization (Q05), about half (56,8%) of the respondents live in the Federal District (DF), and the vast majority (62,2%) are employees of the Public Administration, followed by the Government administration (16,2%). Concerning experience in data privacy (Q04), the largest proportion of respondents (54,1%) have between 1 and 5 years of experience, while almost 92% are in the category of less than 6 years of experience in this area.

With regard to experience with data privacy laws, **Figure 8** shows the results of questions Q06, Q07, and Q08. It can be seen that for both previous experience (see **Figure 8a**) and current experience (see **Figure 8b**), the majority of participants (70,9%) have some knowledge of the guidelines. Regarding the level of experience with the data protection laws, the majority of the participants had a basic (54,1%) or advanced (29,7%) level, as shown in **Figure 8c**.

In addition, the average of the questions about usability and ease of use are shown in **Figure 9**. In order to make it easier to evaluate, the ID of the questions (Q09 – Q17) and their description have also been included. With regard to usability, it can be seen that the majority of the participants agree that the guide is useful both theoretically and practically. Regarding ease of use, a good number of participants also agree with the simplicity of the guide, although some respondents reported that the guide requires a certain level of knowledge of privacy legislation to be fully understood (Q17). Again, the participants' individual responses can be fully verified in Zenodo [Rocha and Canedo, 2024].

Regarding guide strengths (Q18), the topic most cited by the respondents was the ease of understanding and clarity, given that an instrument is proposed that seeks to compare complex legislation while maintaining the clarity of the methodology and providing references. In addition, the participants cited other aspects such as applicability in organizations, interactivity through gamification (principles and rights sections), and raising awareness about the issues dealt with in data privacy.



(a) Participant has previously researched or worked with laws.

(b) Participant currently researches or works with laws.

(c) Participant's level of experience with laws.

Figure 8. Participant profile: experience in data protection laws.

As for the guide's weak points (Q19) and recommended improvements (Q20), the main topic raised by respondents was its possible complexity for beginners. This is due to the fact that the use of terms in the legislation (technical) requires a certain level of prior knowledge. This problem could be mitigated with the introduction of a dictionary of terms in the guide, such as a glossary, in which it would be possible to understand the context of the term used through simple language. Other weaknesses include the lack of a Portuguese version of the guide, generalization, and lack of example use cases.

Table 8 shows the main strengths, weaknesses, and improvements reported by the respondents, in which at least three participants elucidated these topics, as well as examples from the transcripts. Also, as mentioned before, individual responses of the participants regarding guide strengths, weaknesses, and improvements can be fully checked in Zenodo [Rocha and Canedo, 2024].

Regarding guide improvements, minor changes, and three significant additions were made to the guide. With regard to the minor changes, there have been textual corrections and a focus on important terms that do not alter the meaning of the guide but merely make it clearer and easier to read. Furthermore, the phrase "This guide aims to support organizations of various sizes in navigating data privacy regulations, providing essential practices without delving into extensive technical details or sector-specific nuances" was inserted in the Introduction in order to inform the generalization of the

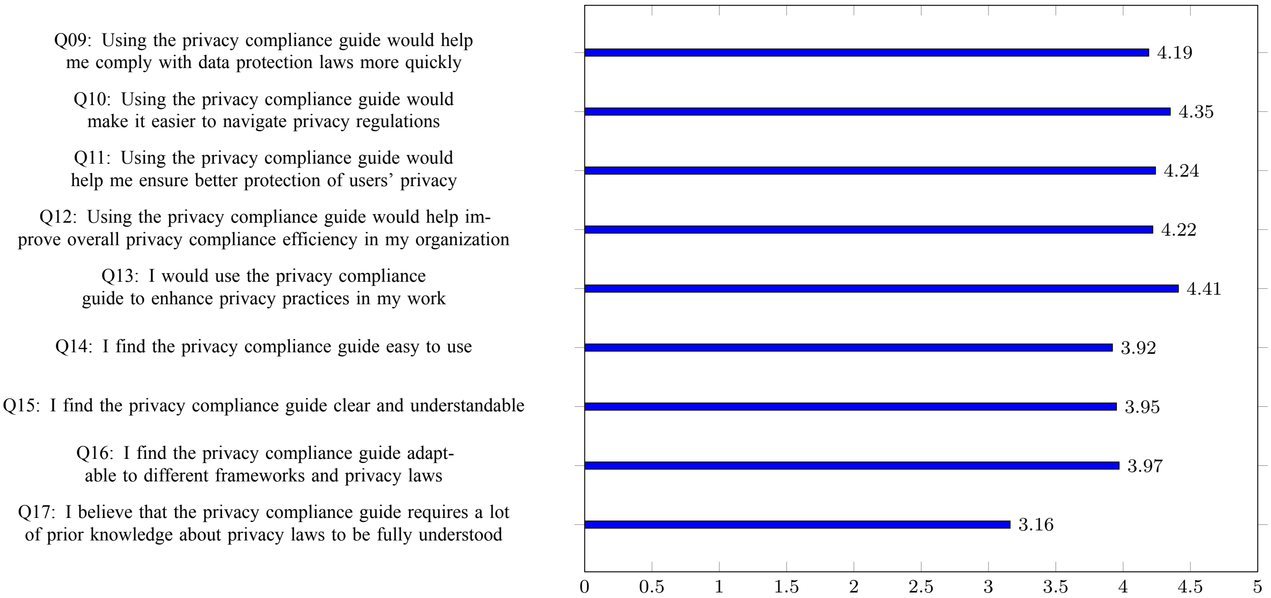


Figure 9. Evaluation of usability and ease of use (Likert scale rating 1–5).

Table 8. Participants' response examples supporting the guide's strengths and weaknesses.

	Construct	**Transcripts**
Strengths	**Clearness and Understandability**	"Ease of information visualization, access to information, and breadth of reference sources." "This innovative approach facilitates the assimilation of content, making learning more dynamic and effective." "Access, easy language and no use of technical terms that make it difficult to understand."
	Applicability	"By directly addressing the challenges organizations face, such as budget constraints and legal ambiguities, the guide becomes a relevant and applicable tool in the daily work of teams." "These strategies help organizations ensure legal compliance and promote a culture of data protection." "The strengths of a privacy compliance guide are: [...] flexibility to adapt, continuous training of employees."
	Interactivity	"The inclusion of an interactive game, which allows users to explore privacy guidelines in a playful way, not only engages participants but also promotes a deeper understanding of how different frameworks can meet legal requirements." "I liked the way the information was presented and the way it interacted with the Principles and Rights tabs." "The possibility of using the cards to select the ISO privacy principles."
	Awareness	"The guide emphasizes education and awareness about privacy, promoting a responsible organizational culture regarding data protection." "The strengths of a private city compliance guide include: [...] Focus on employee education and awareness." "It helps spread the word about the importance of privacy."
	Simplified Access	"[...] it consolidates in one place the information about the key regulations on the subject." "It makes it easier to navigate privacy regulations." "Clear, direct, concise and allows you to quickly compare existing legislation in other countries."
Weaknesses	**Complexity for Beginners**	"The guide also assumes a basic understanding of legal and technical terms, which may be a barrier for non-experts." "User need to understand the differences between countries' laws." "I believe that some of the information could be structured in such a way as to emphasize the LGPD as a starting point."
	Portuguese Version	"There is no option for Portuguese, which is necessary given that it deals with Brazilian regulations." "It could be translated into Portuguese." "As it was a survey applied in Brazil and is also based on the LGPD, I missed the fact that it was not available in Portuguese."
	Generalization	"Generic approach, lacking customization for different types of organizations." "Generic approach, without considering specific needs." "The difficulty of serving all the agencies."
	Examples	"[...] it should include practical examples and case studies." "Include practical real-world examples and case studies of how organizations overcome challenges." "Exemplify/practice."

guide and its intentions.

As for significant additions, the first seeks to solve the problem of high complexity for beginners. To this end, an interactive glossary has been implemented in which, when a user hovers the mouse over very technical terms or terms new to beginners, a box briefly explains what they mean. Then, in the About section, an ongoing example of using the guide was added in order to provide a clear context of how to use the gamification of the guide for everyday situations. Finally, a Brazilian Portuguese version[4] of the guide has also been produced, with its source code available on GitHub[5]. These improvements aim to make the guide a more accessible and useful tool for all audiences.

7 Discussion

Based on the results, a practical and accessible guide was developed for professionals in the field, which complements previous studies that present comparisons between laws and specific challenges. For example, studies such as Canedo *et al.* [2020], Sangaroonsilp *et al.* [2023], and Canedo *et al.* [2022] discuss both comparisons between laws and challenges faced by organizations, but there is a focus on just one area of legislation — principles or rights —, with no in-depth look at compliance techniques or the integration of multiple frameworks.

In addition, studies such as Aljeraisy *et al.* [2022b], Barth *et al.* [2023] and Camêlo and Alves [2023] are much more in line with the proposal of this work in terms of comparison, since they use coding techniques to map requirements. However, the current work differs in that it explores the scope, definitions, and sanctions addressed by the legislation, as well as integrates privacy by design practices and the ISO framework. In this way, the guide seeks to meet the specific needs of developers and their respective organizations by providing practical and detailed guidelines for achieving compliance in an effective and interactive way.

Regarding future concerns, the guide developed for this research may need revisions to remain relevant and effective,

[4] `https://xdalle.github.io/5L2FGuide-PT-BR-`

[5] `https://github.com/xDalle/5L2FGuide-PT-BR-`

as any tool of time volatility. A point of concern is a challenge highlighted by survey respondents, which is the constant changes in the law. Compliance guidelines and frameworks may become insufficient as these laws adapt to respond to emerging problems. Therefore, it would be necessary to include new recommended practices in the guide that align with the new regulatory realities.

7.1 Threats to Validity

The methodology proposed by Wohlin *et al.* [2012] was used to report potential threats to the validity of the study and, consequently, mitigation strategies. Regarding conclusion validity, low statistical power is a major threat for most SLRs since choosing a small number of articles can lead to erroneous conclusions. To mitigate this, in addition to the selection of base studies, snowballing was a good alternative to massify the number of related studies.

Regarding internal validity, the study may present selection bias since not all articles dealing with comparisons between laws and organizations' compliance challenges can be included, and thus, they may have a direct impact on the SLR result. To mitigate this threat, the study selection process was carried out by two people for multiple digital databases, with well-defined inclusion and exclusion criteria — including snowballing — so that there was a wide choice of related articles.

Regarding construct validity, inadequate pre-operational explanation of the constructs threatens the SLR since studies may present similar terms but with different or mistaken definitions. A peer review and subsequent coding of the information was carried out to mitigate this threat, especially in the legislation comparison stage. With regard to the research questions and the SLR protocol, there is no way to guarantee that the selection of synonyms for terms such as "challenges" and "opportunities" was carried out exhaustively. The snowball technique helped reduce this threat, as it broadened the search to include studies that may have used different terminology. There is also a limitation in terms of practical application since, due to time constraints, the lack of case studies or controlled experiments weakens the empirical support for the tool, which could affect the interpretation and application of the results.

Regarding external validity, a major threat to SLR is the interaction between history and treatment. Depending on a study's date of publication and the temporal context, privacy and data protection rules could be more flexible or stricter. To mitigate this threat, the limits of each piece of legislation were highlighted, as well as cultural and historical motivations. Also, the results are limited in their generalizability. The participants' answers will not necessarily serve to generalize the challenges of all developers and organizations, as the major focus on Brazilian law could also affect the elaboration of the guide's strengths and weaknesses.

8 Conclusion

This study carries out a comparative analysis of global data privacy laws (LGPD, GDPR, ADPPA, and Australian Privacy Act) and privacy frameworks (Privacy by Design and ISO/IEC 29100). An SLR identified similarities, differences, challenges, and techniques for both compliance and mitigation. GDPR guidelines are very similar to LGPD, making them the most comprehensive, respectively, while ADPPA focuses more on corporate freedom and Australian Privacy Law has the least comprehensive scope. A survey with developers validated that the lack of knowledge of the law is the biggest challenge, reinforcing the theoretical difficulty. Then, the unified guide was drawn up, incorporating a comparison of the laws, the coverage of the frameworks, and the mapping of the challenges and mitigation techniques. Future studies could strengthen empirical validation through case studies and experimentation in an industrial environment, also it could extend the study to support even more data protection laws.

Declarations

Acknowledgements

This study was financed in part by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Finance Code 001.

Authors' Contributions

Lucas Dalle Rocha conducted the research, data collection, analysis, and writing. Edna Dias Canedo provided supervision, methodological guidance, and critical revisions. Both authors approved the final manuscript.

Competing interests

The authors declare that there are no conflicts of interest.

Availability of data and materials

The supplementary material related to this study is publicly available at Zenodo: `https://doi.org/10.5281/zenodo.14172394` [Rocha and Canedo, 2024].

References

Alhazmi, A. and Arachchilage, N. A. G. (2021). I'm all ears! Listening to software developers on putting GDPR principles into software development practice. *Pers. Ubiquitous Comput.*, 25(5):879–892. DOI: 10.1007/s00779-021-01544-1.

Aljeraisy, A., Barati, M., Rana, O. F., and Perera, C. (2022a). Exploring the relationships between privacy by design schemes and privacy laws: A comparative analysis. *CoRR*, abs/2210.03520. DOI: 10.48550/arXiv.2210.03520.

Aljeraisy, A., Barati, M., Rana, O. F., and Perera, C. (2022b). Privacy laws and privacy by design schemes for the internet of things: A developer's perspective. *ACM Comput. Surv.*, 54(5):102:1–102:38. DOI: 10.1145/3450965.

Almeida, D. R. S., Shmarko, K., and Lomas, E. (2022). The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of us, eu, and UK regulatory frameworks. *AI Ethics*, 2(3):377–387. DOI: 10.1007/s43681-021-00077-w.

Alomar, N. and Egelman, S. (2022). Developers say the darnedest things: Privacy compliance processes followed by developers of child-directed apps. *Proc. Priv. Enhancing Technol.*, 2022(4):250–273. DOI: 10.56553/popets-2022-0108.

Anwar, M. J., Gill, A., and Beydoun, G. (2018). A review of australian information privacy laws and standards for secure digital ecosystems. In *Australasian Conference on Information Systems, ACIS 2018, Sydney, NSW, Australia, 3-5 December 2018*, page 36. Available at:https://aisel.aisnet.org/acis2018/36/.

Ardabili, B. R., Pazho, A. D., Noghre, G. A., Neff, C., Ravindran, A., and Tabkhi, H. (2022). Understanding ethics, privacy, and regulations in smart video surveillance for public safety. *CoRR*, abs/2212.12936. DOI: 10.48550/arXiv.2212.12936.

Ayala-Rivera, V. and Pasquale, L. (2018). The grace period has ended: An approach to operationalize GDPR requirements. In *26th IEEE International Requirements Engineering Conference, RE 2018, Banff, AB, Canada, August 20-24, 2018*, pages 136–146. IEEE Computer Society. DOI: 10.1109/RE.2018.00023.

Barth, S., Ionita, D., and Hartel, P. H. (2023). Understanding online privacy - A systematic review of privacy visualizations and privacy by design guidelines. *ACM Comput. Surv.*, 55(3):63:1–63:37. DOI: 10.1145/3502288.

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

Brodin, M. (2019). A framework for gdpr compliance for small-and medium-sized enterprises. *European Journal for Security Research*, 4:243–264. DOI: 10.1007/s41125-019-00042-z.

Cambraia, D. (2021). Em 2021, Brasil ficou no topo de vazamento de informação no mundo, diz especialista. *CNN.* Available at:https://www.cnnbrasil.com.br/tecnologia/em-2021-brasil-ficou-no-topo-de-vazamento-de-informacao-no-mundo-diz-especialista/.

Camêlo, M. N. and Alves, C. (2023). G-priv: Um guia para apoiar a especificação de requisitos de privacidade em conformidade com a LGPD. *Braz. J. Inf. Syst.*, 16(1). DOI: 10.5753/isys.2023.2743.

Canedo, E. D., Calazans, A. T. S., Bandeira, I. N., Costa, P. H. T., and Masson, E. T. S. (2022). Guidelines adopted by agile teams in privacy requirements elicitation after the brazilian general data protection law (LGPD) implementation. *Requir. Eng.*, 27(4):545–567. DOI: 10.1007/s00766-022-00391-7.

Canedo, E. D., Calazans, A. T. S., Cerqueira, A. J., Costa, P. H. T., and Masson, E. T. S. (2021a). Agile teams' perception in privacy requirements elicitation: Lgpd's compliance in brazil. In *29th IEEE International Requirements Engineering Conference, RE 2021, Notre Dame, IN, USA, September 20-24, 2021*, pages 58–69. IEEE. DOI: 10.1109/RE51729.2021.00013.

Canedo, E. D., Calazans, A. T. S., Masson, E. T. S., Costa, P. H. T., and Lima, F. (2020). Perceptions of ICT Practitioners Regarding Software Privacy. *Entropy*, 22(4):429. DOI: 10.3390/e22040429.

Canedo, E. D., Ribeiro, V. C., de Aguiar Alarcão, A. P., Chaves, L. A. C., Reed, J. N., de Mendonça, F. L. L., and de Sousa Júnior, R. T. (2021b). Challenges regarding the compliance with the general data protection law by brazilian organizations: A survey. In Gervasi, O., Murgante, B., Misra, S., Garau, C., Blecic, I., Taniar, D., Apduhan, B. O., Rocha, A. M. A. C., Tarantino, E., and Torre, C. M., editors, *Computational Science and Its Applications - ICCSA 2021 - 21st International Conference, Cagliari, Italy, September 13-16, 2021, Proceedings, Part III*, volume 12951 of *Lecture Notes in Computer Science*, pages 438–453. Springer. DOI: 10.1007/978-3-030-86970-0_31.

Carvalho, A. P., Canedo, E. D., Carvalho, F. P., and Carvalho, P. H. P. (2020). Anonymisation and compliance to protection data: Impacts and challenges into big data. In *Proceedings of the 22nd International Conference on Enterprise Information Systems, ICEIS 2020, Prague, Czech Republic, May 5-7, 2020, Volume 1*, pages 31–41. SCITEPRESS. DOI: 10.5220/0009411100310041.

Cavoukian, A. (2009). Privacy by design. Available at:https://student.cs.uwaterloo.ca/~cs492/papers/7foundationalprinciples_longer.pdf.

Chun Tie, Y., Birks, M., and Francis, K. (2019). Grounded theory research: A design framework for novice researchers. *SAGE open medicine*, 7:2050312118822927. DOI: 10.1177/2050312118822927.

Daoudagh, S. and Marchetti, E. (2022). The GDPR compliance and access control systems: Challenges and research opportunities. In Mori, P., Lenzini, G., and Furnell, S., editors, *Proceedings of the 8th International Conference on Information Systems Security and Privacy, ICISSP 2022, Online Streaming, February 9-11, 2022*, pages 571–578. SCITEPRESS. DOI: 10.5220/0010912300003120.

Davier, T. S. V., Kollnig, K., Binns, R., Kleek, M. V., and Shadbolt, N. (2023). We are not there yet: The implications of insufficient knowledge management for organisational compliance. *CoRR*, abs/2305.04061. DOI: 10.48550/arXiv.2305.04061.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS quarterly*, pages 319–340. DOI: 10.2307/249008.

de Castro, E. T. V., Silva, G. R. S., and Canedo, E. D. (2022). Ensuring privacy in the application of the brazilian general data protection law (LGPD). In *SAC '22: The 37th ACM/SIGAPP Symposium on Applied Computing, Virtual Event, April 25 - 29, 2022*, pages 1228–1235. ACM. DOI: 10.1145/3477314.3507023.

Doneda, D. (2020). *Da privacidade à proteção de dados pessoais: elementos da formação da lei geral de proteção de* *dados*. Revista dos Tribunais. São Paulo: Thomas Reuters Brasil, 2nd edition. Book.

Ekambaranathan, A., Zhao, J., and Chalhoub, G. (2023). Navigating the data avalanche: Towards supporting developers in developing privacy-friendly children's apps. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, 7(2):53:1–53:24. DOI: 10.1145/3596267.

Ekambaranathan, A., Zhao, J., and Kleek, M. V. (2021). "money makes the world go around": Identifying barriers to better privacy in children's apps from developers' perspectives. In *CHI '21: CHI Conference on Human Factors in Computing Systems, Virtual Event / Yokohama, Japan, May 8-13, 2021*, pages 46:1–46:15. ACM. DOI: 10.1145/3411764.3445599.

European Parliament, T. and Council, T. (2018). General Data Protection Regulation (GDPR): EU Data Protection Rules. Available at:https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

Felizardo, K. R., Mendes, E., Kalinowski, M., de Souza, É. F., and Vijaykumar, N. L. (2016). Using forward snowballing to update systematic reviews in software engineering. In *Proceedings of the 10th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement, ESEM 2016, Ciudad Real, Spain, September 8-9, 2016*, pages 53:1–53:6. ACM. DOI: 10.1145/2961111.2962630.

Feng, Y., Liu, B., Cui, X., Liu, C., Kang, X., and Su, J. (2018). A systematic method on PDF privacy leakage issues. In *17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications / 12th IEEE International Conference On Big Data Science And Engineering, TrustCom/BigDataSE 2018, New York, NY, USA, August 1-3, 2018*, pages 1020–1029. IEEE. DOI: 10.1109/TrustCom/BigDataSE.2018.00144.

Ferrão, S. É. R., Carvalho, A. P., Canedo, E. D., Mota, A. P. B., Costa, P. H. T., and Cerqueira, A. J. (2021). Diagnostic of data processing by brazilian organizations - A low compliance issue. *Inf.*, 12(4):168. DOI: 10.3390/info12040168.

Ferrão, S. É. R., Silva, G. R. S., Canedo, E. D., and Mendes, F. F. (2024). Towards a taxonomy of privacy requirements based on the LGPD and ISO/IEC 29100. *Inf. Softw. Technol.*, 168:107396. DOI: 10.1016/j.infsof.2024.107396.

Freitas, M. d. C. and Mira da Silva, M. (2018). Gdpr compliance in smes: There is much to be done. *Journal of Information Systems Engineering & Management*, 3(4):30. Available at:https://pdfs.semanticscholar.org/5976/4bd60d47803b6b2c9c6d0adc4a53550b539b.pdf.

Goldsmith, L. J. (2021). Using framework analysis in applied qualitative research. *Qualitative Report*, 26(6). DOI: 10.46743/2160-3715/2021.5011.

Hornuf, L., Mangold, S., and Yang, Y. (2023). Data protection law in germany, the united states, and china. In *Data Privacy and Crowdsourcing: A Comparison of Selected Problems in China, Germany and the United States*, pages 19–79. Springer. DOI: 10.1007/978-3-031-32064-4$_3$.

Horstmann, S. A., Domiks, S., Gutfleisch, M., Tran, M., Acar, Y., Moonsamy, V., and Naiakshina, A. (2024). "those things are written by lawyers, and programmers are reading that." mapping the communication gap between software developers and privacy experts. *Proc. Priv. Enhancing Technol.*, 2024(1):151–170. DOI: 10.56553/popets-2024-0010.

ISO Central Secretary (2011). ISO/IEC 29100 : Information technology — security techniques — privacy framework. Standard, International Organization for Standardization, Geneva, CH. Available at:https://www.iso.org/standard/85938.html.

Kaufmann, J., Hilgert, F., and Wohlthat, R. (2022). The proposed american data privacy and protection act in comparison with gdpr. *Computer Law Review International*, 23(5):146–152. DOI: 10.9785/cri-2022-230505.

Kitchenham, B., Charters, S., *et al.* (2007). Guidelines for performing systematic literature reviews in software engineering. Available at:https://www.researchgate.net/profile/Barbara-Kitchenham/publication/302924724_Guidelines_for_performing_Systematic_Literature_Reviews_in_Software_Engineering/links/61712932766c4a211c03a6f7/Guidelines-for-performing-Systematic-Literature-Reviews-in-Software-Engineering.pdf.

Kühtreiber, P., Pak, V., and Reinhardt, D. (2022). A survey on solutions to support developers in privacy-preserving iot development. *Pervasive Mob. Comput.*, 85:101656. DOI: 10.1016/j.pmcj.2022.101656.

Li, Z. S., Werner, C. M., Ernst, N. A., and Damian, D. E. (2020). GDPR compliance in the context of continuous integration. *CoRR*, abs/2002.06830. DOI: 10.48550/arXiv.2002.06830.

Li, Z. S., Werner, C. M., Ernst, N. A., and Damian, D. E. (2022). Towards privacy compliance: A design science study in a small organization. *Inf. Softw. Technol.*, 146:106868. DOI: 10.1016/j.infsof.2022.106868.

Lorenzon, L. N. (2021). Análise comparada entre regulamentações de dados pessoais no Brasil e na União Europeia (LGPD e GDPR) e seus respectivos instrumentos de enforcement. *Centro de Excelência Jean Monnet da FGV Direito Rio*. Available at:https://periodicos.fgv.br/rpdue/article/view/83423.

Machado, P., Vilela, J., Peixoto, M. M., and Silva, C. T. L. L. (2023). A systematic study on the impact of GDPR compliance on organizations. In *Proceedings of the XIX Brazilian Symposium on Information Systems, SBSI 2023, Maceió, Brazil, 29 May 2023- 1 June 2023*, pages 435–442. ACM. DOI: 10.1145/3592813.3592935.

Matulytė, R. (2022). *Comparing data protection regulation models of the eu and the us: which one is more preferred by the society?* PhD thesis. Available at:https://epublications.vu.lt/object/elaba:175679457/.

Naqvi, S. K. H. and Batool, K. (2023). A comparative analysis between general data protection regulations and california consumer privacy act. *Journal of Computer Science, Information Technology and Telecommunication Engineering*, 4(1):326–332. DOI: 10.30596/jcositte.v4i1.13330.

Neves, R. d. A. P. (2021). GDPR e LGPD: Estudo comparativo. Available at:https://repositorio.uniceub.br/jspui/handle/prefix/15239.

Nurgalieva, L., Frik, A., and Doherty, G. (2023). A narrative review of factors affecting the implementation of privacy and security practices in software development. *ACM Comput. Surv.*, 55(14s). DOI: 10.1145/3589951.

OAIC, A. G. (1988). The Privacy Act. Available at:https://www.oaic.gov.au/privacy/privacy-legislation/the-privacy-act.

Park, G. (2019). The changing wind of data privacy law: A comparative study of the european union's general data protection regulation and the 2018 california consumer privacy act. *UC Irvine L. Rev.*, 10:1455. Available athttps://escholarship.org/uc/item/8562f0v0.

Peixoto, M. M., Ferreira, D., Cavalcanti, M., Silva, C., Vilela, J., Araújo, J., and Gorschek, T. (2020). On understanding how developers perceive and interpret privacy requirements research preview. In *Requirements Engineering: Foundation for Software Quality - 26th International Working Conference, REFSQ 2020, Pisa, Italy, March 24-27, 2020, Proceedings [REFSQ 2020 was postponed]*, volume 12045 of *Lecture Notes in Computer Science*, pages 116–123. Springer. DOI: 10.1007/978-3-030-44429-7_8.

Pires, F., Pacheco, O. R., and Martins, R. T. (2021). Why you should care about gdpr in iot enterprises & solutions. In *2021 16th Iberian Conference on Information Systems and Technologies (CISTI)*, pages 1–9. IEEE. DOI: 10.23919/CISTI52073.2021.9476614.

Pitogo, V. A. and Ching, M. R. D. (2018). Understanding philippine national agency's commitment on data privacy act of 2012: a case study perspective. In *Proceedings of the 2nd International Conference on E-commerce, E-Business and E-Government, ICEEG 2018, Hong Kong, SAR, China, June 13-15, 2018*, pages 64–68. ACM. DOI: 10.1145/3234781.3234788.

Poritskiy, N., Oliveira, F., and Almeida, F. (2019). The benefits and challenges of general data protection regulation for the information technology sector. *Digital Policy, Regulation and Governance*, 21(5):510–524. DOI: 10.1108/dprg-05-2019-0039.

Rocha, L. D. and Canedo, E. D. (2024). Supplementary Material for Comparative Analysis of Data Protection Laws and Privacy Frameworks: Optimizing Solutions for Compliance with LGPD and International Data Sharing Laws. Available at:https://zenodo.org/records/14172394.

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: .1145/3555776.3577615.

Sangaroonsilp, P., Dam, H. K., Choetkiertikul, M., Ragkhitwetsagul, C., and Ghose, A. (2023). A taxonomy for mining and classifying privacy requirements in issue reports. *Inf. Softw. Technol.*, 157:107162. DOI: 10.1016/j.infsof.2023.107162.

Selim, A. (2021). Systematic review of big data, digital transformation areas and industry 4.0 trends in 2021. *International Scientific Journal Vision*, 6(2):27–41. Available at: https://visionjournal.edu.mk/social/index.php/1/article/view/98/98.

Sirur, S., Nurse, J. R. C., and Webb, H. (2018). Are we there yet?: Understanding the challenges faced in complying with the general data protection regulation (GDPR). In *Proceedings of the 2nd International Workshop on Multimedia Privacy and Security, MPS@CCS 2018, Toronto, ON, Canada, October 15, 2018*, pages 88–95. ACM. DOI: 10.1145/3267357.3267368.

State of California, D. o. J. (2018). California consumer privacy act. Available at:https://oag.ca.gov/privacy/ccpa.

Tahaei, M., Frik, A., and Vaniea, K. (2021). Privacy champions in software teams: Understanding their motivations, strategies, and challenges. In *CHI '21: CHI Conference on Human Factors in Computing Systems, Virtual Event / Yokohama, Japan, May 8-13, 2021*, pages 693:1–693:15. ACM. DOI: 10.1145/3411764.3445768.

Teixeira, G. A., da Silva, M. M., and Pereira, R. (2019). The critical success factors of gdpr implementation: a systematic literature review. *Digital Policy, Regulation and Governance*, 21(4):402–418. DOI: 10.1108/DPRG-01-2019-0007.

U.S. Congress, C. o. E. and Commerce (2022). American Data Privacy and Protection Act (ADPPA). Available at: https://www.congress.gov/bill/117th-congress/house-bill/8152/text.

Voss, W. G. (2021). The ccpa and the gdpr are not the same: why you should understand both. *W. Gregory Voss,'The CCPA and the GDPR Are Not the Same: Why You Should Understand Both,'CPI Antitrust Chronicle*, 1(1):7–12. Available at: https://hal.science/hal-03116018v1.

Weber, P. A., Zhang, N., and Wu, H. (2020). A comparative analysis of personal data protection regulations between the EU and china. *Electron. Commer. Res.*, 20(3):565–587. DOI: 10.1007/s10660-020-09422-3.

Wiefling, S., Tolsdorf, J., and Iacono, L. L. (2022). Data protection officers' perspectives on privacy challenges in digital ecosystems. In Katsikas, S. K., Cuppens, F., Kalloniatis, C., Mylopoulos, J., Pallas, F., Pohle, J., Sasse, M. A., Abie, H., Ranise, S., Verderame, L., Cambiaso, E., Vidal, J. M., Monge, M. A. S., Albanese, M., Katt, B., Pirbhulal, S., and Shukla, A., editors, *Computer Security. ESORICS 2022 International Workshops - CyberICPS 2022, SECPRE 2022, SPOSE 2022, CPS4CIP 2022, CDT&SECOMANE 2022, EIS 2022, and SecAssure 2022, Copenhagen, Denmark, September 26-30, 2022, Revised Selected Papers*, volume 13785 of *Lecture Notes in Computer Science*, pages 228–247. Springer. DOI: 10.1007/978-3-031-25460-4_13.

Wohlin, C., Runeson, P., Höst, M., Ohlsson, M. C., Regnell, B., and Wesslén, A. (2012). *Experimentation in software engineering*. Springer Science & Business Media. DOI: 10.1007/978-3-662-69306-3.

Wong, R. Y., Chong, A., and Aspegren, R. C. (2023). Privacy legislation as business risks: How GDPR and

CCPA are represented in technology companies' investment risk disclosures. *Proc. ACM Hum. Comput. Interact.*, 7(CSCW1):1–26. DOI: 10.1145/3579515.