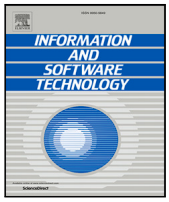
Information and Software Technology 168 (2024) 107396

Contents lists available at ScienceDirect

Information and Software Technology

journal homepage: www.elsevier.com/locate/infsof



Towards a taxonomy of privacy requirements based on the LGPD and ISO/IEC 29100

Sâmmara Éllen Renner Ferrão [a], Geovana Ramos Sousa Silva [b], Edna Dias Canedo [b,a,*], Fabiana Freitas Mendes [b]

[a] University of Brasilia (UnB), Technology College, Electrical Engineering Department (ENE), Brasilia, DF, Brazil
[b] University of Brasilia (UnB), Department of Computer Science, Brasilia, DF, Brazil

ARTICLE INFO

Dataset link: https://zenodo.org/doi/10.5281/zenodo.6590218

Keywords:
Privacy requirements elicitation
Taxonomy
LGPD
ISO/IEC2900
Compliance

ABSTRACT

Context: Ensuring compliance with current data privacy legislation poses a significant challenge for software development teams, demanding adaptations to processes in order to align with legal requirements.
Objective: This study proposes a comprehensive taxonomy of privacy requirements, drawing from the Brazilian General Data Protection Law (LGPD) and ISO/IEC 29100. The aim is to assist software development teams in navigating the complexities of legal compliance.
Method: To define the research gap, we conducted a systematic literature review (SLR) initially, identifying existing taxonomies of privacy requirements. Subsequently, we applied the Goal-Based Requirements Analysis Method (GBRAM) to extract privacy requirements from LGPD and ISO/IEC 29000. Finally, we implemented the proposed taxonomy in the privacy policies of Brazil's three largest banks.
Results: The taxonomy comprises 129 requirements, categorized into 10 distinct groups across 5 contexts. In applying the taxonomy to ISO/IEC 29100, analysis of 63 statements for GDPR+ISO/IEC 29100 yielded 33 requirements, whereas for LGPD+ISO/IEC 29100, 58 statements resulted in 57 requirements. Application of the taxonomy revealed adherence percentages ranging from 40% to 71% concerning the evaluated solutions.
Conclusions: The outcomes strongly suggest that major corporations are yet to achieve full LGPD compliance. We posit that the proposed taxonomy offers a valuable industry tool for validating LGPD compliance within implemented systems, as exemplified by our successful use case with Brazilian banks.

1. Introduction

With the increasing amount of data generated and stored today and with the awareness of users about the importance of their data since the advent of the Brazilian Internet Bill of Rights (in Brazilian Portuguese *Marco Civil da Internet* - MCI) [1], data privacy has become necessary and meaningful to data subjects. Nevertheless, users' concerns are enhanced by the recent data leakage events [2–5], which evidence the need to ensure the protection of their personal data, especially in the Brazilian scenario where only 20% of Brazilian organizations have established communication processes about possible leaks of personal data [6] and only 23% perform incident management to effectively deal with possible data leaks [6].

The Brazilian General Data Protection Law (LGPD) [7] was published on 14th August 2018, and came into force 24 months after its publication. LGPD aims to regulate the use of personal data, protect the fundamental rights of freedom and privacy, and the free development of the personality of individuals [7]. Therefore, any person or institution that performs any kind of personal data treatment in activities carried out within the Brazilian territory is obliged to comply with this law. The wording of the LGPD was inspired by the General Data Protection Regulation (GDPR) [8], the European legislation to regulate the protection of personal data in Europe, which makes both laws share some similarities.

In the context of Software Engineering, in which technical and management efforts are used to transform a set of needs into solutions [9], Requirements Engineering is an area that demands great attention in working through regulatory standards, as it is responsible for identifying, specifying, validating and managing the functional and non-functional requirements [10–12]. Non-functional requirements describe how the system should behave, and since they are more complex and difficult to elicit, they end up not receiving the necessary priority or even not being fully executed [13] during the identification, analysis, and specification phase of requirements.

* Corresponding author.
E-mail address: ednacanedo@unb.br (E. Dias Canedo).

https://doi.org/10.1016/j.infsof.2024.107396
Received 14 June 2023; Received in revised form 8 November 2023; Accepted 3 January 2024
Available online 6 January 2024

Negligence is considered one of the biggest problems related to non-functional requirements [13–16]. Some authors mentioned that these requirements are commonly described incompletely, [17–19] making the analysis, development, and consequently, the testing of functionalities more difficult [17–20]. Since privacy requirements are categorized as non-functional requirements, they end up inheriting the challenges of it.

As privacy requirements can be used to record requirements based on legal bases, this context makes it difficult to elicit these requirements as it is an activity generally performed by requirements engineers/analysts who do not have experience in interpreting legal standards [21–24]. Ansari et al. [25] highlighted that correctly identifying and modeling privacy requirements during the software development phase is essential for delivering software with a significant level of protection for user's data privacy. There are four types of privacy requirements [24], namely: compliance, access control, verification, and usability. The compliance type addresses the principles established by the LGPD.

Guzmán et al. [26] stated that non-functional requirements play an important role in the success of software systems. In this sense, there is a need for a practical approach to eliciting privacy requirements in the context of legal regulations and security and privacy frameworks. Thus, to meet this challenge of a practical approach to eliciting privacy requirements, in this work, we propose a taxonomy in the context of privacy requirements based on GDPR and ISO/IEC 29100.

There are some works in the literature about privacy requirements taxonomies [27–31], one specifically with a more comprehensive purpose and based on legal regulation. Sangaroonsilp et al. [32] address a taxonomy specifically of privacy requirements in the context of the GDPR, the European legislation about data privacy. To our knowledge, there is no such work that proposes a taxonomy based on the LGPD, the Brazilian law, and representative of all kinds of software systems.

The GDPR and LGPD, while sharing many similarities, can pose legal challenges for organizations using software developed for other laws. This is because variations in the Brazilian law may be overlooked. The LGPD, designed for the Brazilian data processing landscape, addresses issues stemming from major data leaks events (2011 – Law No. 12,527, Access to Information Law; 2012 – Law No. 12,737, Carolina Dieckmann Law). Unlike the GDPR with 6 chapters, the LGPD has 10 chapters and offers a more comprehensive vision on data treatment and privacy. It establishes the National Data Protection Authority (ANPD) for supervision and sanctions, while GDPR has all supervision and sanction determinations in its own text of the Law. Existing taxonomies for the GDPR may not be suitable for Brazilian organizations, necessitating the development of a specific taxonomy for the LGPD. Therefore, the related works that propose taxonomies for the GDPR do not meet the needs of Brazilian organizations, as it is necessary to develop a specific taxonomy for the LGPD.

In this research, we performed a reproduction of the steps proposed by [32] for the creation of a taxonomy of privacy requirements based on LGPD and ISO/IEC 29100 for the Brazilian context. The LGPD was chosen considering that it is the general law for the protection of personal data that gives Brazilians the right to protect their data, being a law that subjectively transcribes various aspects of privacy. Likewise, ISO/IEC 29100 was also chosen due to being a reference framework for security and data privacy.

As a result of this research, a taxonomy with 129 privacy requirements is presented to support software development teams in the activity of eliciting privacy requirements in accordance with LGPD and ISO/IEC 29100. The taxonomy can be considered as a guideline for Information and Communication Technology (ICT) practitioners to base themselves on during the elicitation and specification of requirements since previous works indicate low compliance with the LGPD law requirements [33], demonstrating that studies approaching this theme are critical to the Brazilian community.

Taxonomies can facilitate implicit requirements identification, as seen in our application in the open banking context, where we found a possibility to increase compliance and it is noticeable that the taxonomy can help reach broader compliance with the LGPD. Thus, the main contribution of this work is a taxonomy of privacy requirements based on LGPD and ISO/IEC 29100 to support software development teams in adapting/conforming to the principles of Brazilian legislation. They can use the taxonomy during the elicitation process as a guideline to identify the compliance main points to their system as well as they can use the taxonomy to analyze compliance in a system already implemented.

This work is organized as follows: Section 2 presents core background knowledge underlying our proposal, Section 3 details the methodology used to carry out our work, Section 4 presents the results of the systematic literature review, Section 5 depicts the proposed taxonomy, Section 6 presents the taxonomy application and its outcomes, Section 7 discusses the findings resulting from this study, Section 8 details the threats to this study's validity, and finally, Section 9 concludes this work. For reference, below are the definitions of important acronyms referenced throughout this work:

- GDPR — General Data Protection Regulation: European regulation on privacy and protection of personal data;
- LGPD — Lei Geral de Proteção de Dados [General Data Protection Law]: Brazilian regulation on privacy and protection of personal data;
- ISO/IEC 29100 — International Organization of Standardization/International Electrotechnical Commission 29100: standard that provides a privacy framework;
- GBRAM — Goal-Based Requirements Analysis Method: a requirements engineering methodology used in this work;
- TAAF — Taxonomy Adherence Assessment Form: form developed in this work to aid the evaluation of conformity to the proposed requirements.

2. Background

2.1. General data protection regulation (GDPR)

The General Data Protection Regulation (GDPR) [8] is the European Union's data protection law that emerged as a replacement and evolution of the Data Protection Directive 95/46/EC (DIR95) [34] and was approved in May 2016. According to [35], the GDPR aims to improve the level of protection and harmonization of personal data by the European Union since DIR95 no longer meets the privacy requirements demanded by the digital environment. The GDPR, which came into force in May 2018, applies to any and all institutions that process data on European Union nationals regardless of physical location. It consists of 99 articles, and its principles are Lawfulness, Fairness and Transparency, Purpose Limitation, Data Minimization, Accuracy, Storage Limitation, Integrity, Confidentiality, and Accountability [8].

The GDPR establishes fines and penalties for security breaches that can be classified according to a catalog of breaches made available by the regulator [36]. For less serious violations, the fines are up to 10 million euros or to 2% of the organization's global turnover. For particularly serious violations, the fine can be up to 20 million euros or up to 4% of turnover.

2.2. Brazilian general data protection law (LGPD)

The General Data Protection Law (LGPD) [7] is the Brazilian law for the protection of personal data that was inspired by the GDPR. After the Brazilian Internet Bill of Rights [1] in 2014, the need for data protection arose, since the indiscriminate processing of data can lead to events of data leaks [2–4] which culminate in the LGPD. With this legislation in force, Brazil has started to be part of a group of more than half of

the countries in the world that have laws for the protection of personal data. According to data from the intergovernmental organization linked to the United Nations [37], in September 2020, 66% of countries in the world have some legislation related to data protection, and privacy, whereas 19% have no legislative initiative in this regard and 10% are in the process of drafting legislation.

The Brazilian law consists of 64 articles and 10 principles related to data processing: Purpose, Suitability, Necessity, Free Access, Data Quality, Transparency, Security, Prevention, Non-Discrimination, and Accountability [7]. The general idea of the law is to protect personal data, establish fundamental rights of freedom and privacy, and the free development of the personality of the individuals [7]. The legislation also establishes that data processing may be carried out by private law institutions as long as consent is requested from the data subject. This consent must indicate a specific purpose. Therefore, generic authorizations and vices of consent are not allowed. Processing agents who do not comply with the requirements for data processing may be punished with administrative sanctions that include making the infringement public after it has been ascertained and confirmed, suspension of the processing exercise referred to in the infringement, fines of up to 2% of the company turnover limited to 50 million reals per infraction, among others [7].

The law has been applied, and considering the current public cases, there are four final cases (final stage of a legal process) that were applied fines and sanctions based exclusively on LGPD [38]. Of the ongoing processes, the sector with the highest number of violations is the banking sector [38]. These violations demonstrate the importance of developing initiatives to support organizations in their pursuit of LGPD compliance.

2.3. ISO/IEC 29100

ISO/IEC 29100 is a framework that aims to establish standards for Information and Communication Technology (ICT) systems to achieve the privacy of personal data. Its approach is focused on organizational, technical, and procedural aspects in a comprehensive privacy framework [39]. The importance of the framework is highlighted by the increase in the processing of personal data and the need for security standards that establish a common understanding for the protection of personal data [39].

The scope of ISO/IEC 29100 includes the definition of common terminology for privacy terms, the definition of actors and their roles in the data processing process, a description of requirements for privacy safeguards, and references to its own 11 privacy principles. The privacy principles of ISO/IEC 29100 are: 1. Consent and choice; 2. Purpose legitimacy and specification; 3. Collection limitation; 4. Data minimization; 5. Use, retention and disclosure limitation; 6. Accuracy and quality; 7. Openness, transparency, and notice; 8. Individual participation and access; 9. Accountability; 10. Information security; and 11. Privacy compliance [39]. Moreover, ISO/IEC 29100 introduces privacy safeguard requirements, a set of requirements that an organization needs to consider when processing personal data in relation to protecting the privacy of personal data [39].

The principles of ISO/IEC 29100 help with the requirements related to the processing of personal data, software development lifecycle, controls for data controllers, and controls for data operators. Thus, ISO/IEC 29100 helps to define the requirements for safeguarding personal data within an ICT environment, specifying a common privacy terminology, defining actors and their roles in processing personal data, describing privacy safeguard requirements, and referencing known privacy principles. These privacy safeguard requirements can be understood as complementary to the legal requirements of the LGPD. Due to the growing number of technologies that process personal data, it is important to have information security standards that provide a common understanding base for protecting it.

Organizations are motivated to protect personal data for a variety of reasons, such as meeting legal and regulatory requirements, practicing corporate responsibility, and increasing consumer confidence. Privacy safeguard requirements can relate to many aspects of personal data processing, such as the collecting and retention of personal data, transferring personal data to third parties, the contractual relationship between data controllers and data operators, and exchanging personal data in between countries.

Privacy safeguard requirements can also vary in specificity and can be very general in nature because of the high-level enumeration of privacy principles. However, privacy safeguard requirements may also contain very specific restrictions on processing certain types of personal data or may require the implementation of specific privacy controls. In summary, ISO/IEC 29100 helps in the performance, implementation, operation, and maintenance of ICT systems that handle and protect personal data; encourages innovative solutions that protect personal data in ICT systems; and improves organizations' privacy programs through the use of best practices.

2.4. Data privacy

The concept of data privacy, in general, can be considered subjective. Different meanings can be attributed to different types of people, however, the perspective that privacy is a human right that depends on the context and the environment inserted, is common to all interpretations [40]. Kaloniatis et al. [41] consider that users' privacy can be defined as the right to determine when data will be used, how they will be used and treated as well as for what purpose [42]. Canedo et al. [22] highlighted that data privacy comprehends user data created by the user or third parties, its use through observations and analysis by individuals, among other items.

Privacy issues have evolved over time, mainly due to the fast evolution of data processing [43]. Finkelstein and Finkelstein [44] consider that technological evolution is a milestone in the history of privacy, as well as the advent of the media, the development of the internet, and the emergence of social networks. Brito and Machado [45] state that data privacy has a barrier to its existence in the technological world due to the high volume and speed of information flow, making the concern with data privacy even more relevant in the information technology context.

2.5. Privacy requirements

According to [46], the definition of privacy requirements is a requirement capable of conveying privacy objectives and the measures associated with those objectives for a given system. Due to this subjective nature, privacy requirements are generally categorized as non-functional requirements and, therefore, end up sharing the same challenges identified in the literature to elicit requirements [13–20].

As in their nature, privacy requirements can be used to comply with legal bases. This primarily legal context can make elicitation difficult as it is generally performed by requirements analysts, systems analysts, and software engineers who do not have experience interpreting legal norms [21–24]. Furthermore, privacy requirements sometimes end up being confused as part of security rather than a specific objective of ensuring privacy [41,47–49], which reduces their real applicability in systemic contexts. Ansari et al. [25] highlighted that the correct identification and modeling of privacy requirements during the software development phase is essential to deliver software with a significant degree of user data privacy protection.

Hadar et al. [50] mentioned that systematic approaches for specifying privacy requirements are an imminent necessity considering that software engineers often lack the necessary knowledge and understanding of privacy concepts to perform requirements elicitation activities.

2.6. Related works

Aberkane et al. [51] provide a viable means of automating GDPR compliance by using natural language processing (NLP). In order to reach such a goal, the authors first conducted a systematic literature review (SLR) which aimed to explore the existing literature on the intersection of GDPR, NLP, and Requirements Engineering (RE). The SLR results indicated opportunities to fill the gap mentioned in the convergence of these three themes. As a result, the authors highlighted the importance of identifying possibilities for the introduction of NLP techniques in the automation of manual requirements engineering tasks and the possibilities of using NLP-based machine learning techniques to achieve GDPR compliance in requirements engineering. The authors' work differs from this project by addressing the possibility of automation in requirements gathering.

Alves and Neves [4] established an empirical analysis of privacy issues by elaborating privacy standard proposals following a qualitative research guide and Ground Theory. This analysis was carried out from semi-structured interviews (27 Questions) with professionals from public organizations with more than 10 years of experience. The interviews revealed some points of perspective that can help IT professionals in the elicitation of privacy requirements and in the creation of privacy standards. This work differs from the work by Alves and Neves by proposing a taxonomy of privacy requirements. Furthermore, Alves and Neves only addressed the empirical analysis of the difficulties in eliciting privacy requirements.

Kanwal et al. [27] developed the E-Health Cloud system. The main issues addressed by the authors were related to finding the most desirable trade-off between privacy preservation and utility using different combinations of privacy models and techniques. The authors also identified the most relevant privacy techniques for cloud-based applications in the e-Health context and proposed a taxonomy for privacy preservation. This work differs from our research because its application is limited to privacy preservation in cloud-based environments.

Meis et al. [30] developed a taxonomy of transparency requirements based on ISO/IEC 29.000 [39] and the draft of the EU Data Protection Regulation, as GDPR [8] had not yet been published. This taxonomy was intended to provide software engineers with a method to identify transparency requirements. They analyzed the description of ISO/IEC 29.000's privacy principles and the draft of the GDPR in order to propose thirty transparency requirements. The evaluation was performed by comparing other taxonomies found in a Systematic Literature Review. Meis et al.'s work differ from ours because it focuses on transparency and non-privacy requirements. Moreover, it is based on a draft of the GDPR, whereas the LGPD was already approved in 2018.

Works prior to the publication of the GDPR already addressed the need for taxonomies [29,31,52–54]. In the scope of the Internet of Things (IoT), [31] presented a taxonomy of security and privacy requirements for (IoT). The authors stated that obtaining privacy and security requirements in a project design phase is crucial for creating a link with the public in order to develop a satisfactory public trust, facilitating the adaptation of these IoT systems. To create the taxonomy, the authors used the structure proposed by [55], which provides a basis for reorganizing security requirements. Our research differs from the work proposed by [55] because the author focused only on security requirements in IoT environments.

Barker et al. [29] highlighted the importance of privacy for the database systems community. The authors provided an explicit definition of data privacy suitable for Database Management Systems (DBMS) and data mining and proposed a taxonomy capable of approaching data privacy technologically. The main contribution highlighted by the authors is a definition of privacy. Barker et al.'s work differs from the approach of our work since the authors used definitions from the literature. In addition, their focus is on DBMS whereas, in this work, the LGPD [7] is considered as the basis for creating our taxonomy.

Massey et al. [28] performed a comparison between an engineering taxonomy of privacy protection requirements and vulnerabilities with a taxonomy of legal privacy damages. The methodological approach for comparison consisted of comparing each vulnerability in the Antón-Earp Taxonomy with each category of legal privacy damages in the Solove Taxonomy and determining whether the vulnerability could reasonably be interpreted as being a subset, a superset, or completely unrelated to each other. As a result, six of the seven vulnerabilities in the Antón-Earp taxonomy were mapped to at most two categories of privacy harm, thus, suggesting a reasonable similarity between these two taxonomies. Barker et al.'s research differs from this project by using a legal taxonomy as a basis for the comparative process, although the Antón-Earp is used as a basis for the article by [32].

The taxonomy proposed in [32] provides a comprehensive set of privacy requirements based on four well-established personal data protection regulations and privacy frameworks. For the development of this taxonomy, GBRAM techniques and grounded theory were used with a 3-step method to obtain the requirements that resulted in a list of seven categories with a total of 71 privacy requirements and 7 goal categories. All requirements identified in the ISO/IEC 29100 were covered by those found in GDPR. This taxonomy was used to develop this work's proposal based on the LGPD and ISO/IEC 29100.

Canedo et al. [33] investigate how Brazilian organizations modified their software development process to implement LGPD privacy requirements. They conducted an online survey with 53 ICT practitioners from different organizations in Brazil and 10 semi-structured interviews with practitioners from agile software development teams. The authors concluded that agile teams face several challenges in eliciting privacy requirements due to the lack of processes, standards or taxonomies to elicit privacy requirements in compliance with the law. Thus, the taxonomy proposed by our work to elicit privacy requirements will minimize the gap pointed by Canedo et al. supporting professionals in the execution of this activity and providing mechanisms to guarantee Brazilian organizations comply with the LGPD.

3. Methodology

This work was conducted using a mixed-methods approach, as illustrated in Fig. 1, comprising three key steps: (1) a systematic literature review (SLR) to delineate the research scope by identifying the research gap; (2) the proposal of a taxonomy employing the Goal-Based Requirements Analysis Method (GBRAM) and Grounded Theory (GT); and (3) the application of the proposed taxonomy to three of the largest banks in Brazil. The subsequent sections provide detailed explanations of each of these steps.

3.1. SLR

Initially, we conducted a systematic literature review (SLR) to identify existing works proposing a taxonomy of privacy requirements and to define the research gap. Although there was already an established intention to replicate the study by Sangaroonsilp et al. [32], the SLR was necessary to ensure that our research goal had not been achieved previously. Additionally, it served the purpose of reviewing related works to gain a comprehensive understanding of the research field.

In order to synthesize and evaluate existing literature on taxonomies of privacy requirements, we will employ a systematic review methodology (SLR). Systematic reviews are recognized as valuable tools for summarizing and analyzing the current state of knowledge in a specific field [56]. This section outlines the steps involved in conducting a systematic review – planing, conducting, and reporting – adhering to the guidelines and best practices recommended by Kitchenham and Charters [56]:

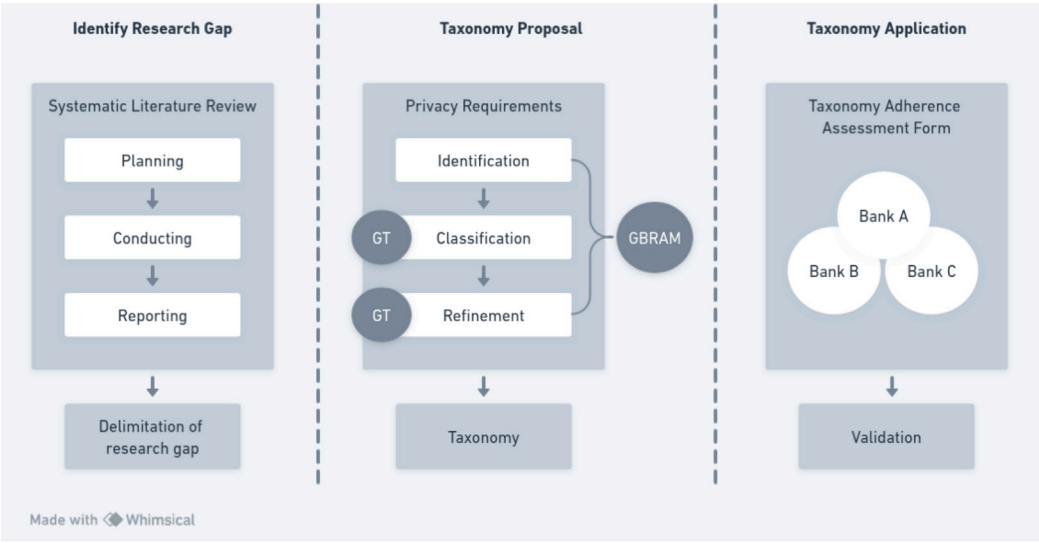


Fig. 1. Research methodology.

1. **Planning:** Meticulously define the research question, laying the foundation for a focused and relevant systematic review. This involves identifying key themes, concepts, or variables to build the search string that will guide the literature search. Additionally, establish explicit inclusion and exclusion criteria, ensuring the systematic selection of studies and minimizing bias, and a quality assessment checklist to evaluate the methodological soundness and relevance of each included study.
2. **Conducting:** Execute a comprehensive literature search utilizing electronic databases, academic repositories, and various sources. The systematic approach employed during this phase aims to identify all relevant studies related to our research question. Independently assessing study eligibility and extracting data according to predefined criteria ensures a transparent and unbiased selection process. Quality assessment is integrated into this phase, with a rigorous evaluation of the methodological robustness and relevance of each included study. The conducting phase emphasizes the systematic and unbiased gathering of information.
3. **Reporting:** Dedicated to presenting our findings in a clear and comprehensive manner, ensuring that our systematic review contributes to the existing body of knowledge on taxonomy of privacy requirements.

3.2. Taxonomy proposal

We employed the Goal-Based Requirements Analysis Method (GBRAM) [32,52,57] to extract privacy requirements that constitute the proposed taxonomy. While Sangaroonsilp et al. [32] applied GBRAM in the development of a taxonomy based on the GDPR [8] and ISO/IEC 29000 [39], this work applies the method to extract requirements from the LGPD [7] and ISO/IEC 29000 [39]. The processes of classifying and refining the privacy requirements were employed through the Grounded Theory methodology.

The Goal-Based Requirements Analysis Method (GBRAM) [57] is used to identify, elaborate, refine, and organize objectives for specifying requirements. GBRAM was utilized by Anton [52] in the development of the requirements taxonomy to reduce vulnerabilities in websites. It was also employed in the development of the taxonomy of privacy requirements proposed by Sangaroonsilp et al. [32], which is based on GDPR and ISO/IEC 29100.

Grounded Theory is a qualitative research methodology developed by sociologists Barney Glaser and Anselm Strauss [58]. It involves three main coding techniques: open coding, axial coding, and selective coding. Open coding is the initial stage where researchers analyze data line by line, assigning conceptual labels to capture the essence of the information. Axial coding follows, aiming to identify connections between different codes and categories, allowing for the exploration of relationships and patterns within the data. Finally, selective coding focuses on refining the core category and developing a comprehensive theory by selecting the most significant codes and their relationships.

Nickerson et al. [59] defined a taxonomy as a grouping of concepts into dimensions composed of two or more characteristics each. For the development of our taxonomy, the LGPD [7] and ISO/IEC 29100 were used as a taxonomic basis. The LGPD guarantees the rights of the natural person in relation to the processing of their data and establishes principles for data treatment, including punishments for irregularities identified by processing agents [7]. ISO/IEC 29100 [39], in turn, is a framework widely known for defining models intended for data protection during its treatment.

As noted by Nickerson et al. [59], a taxonomy requires classification into dimensions. Therefore, the dimensions assigned to our taxonomy are the LGPD principles: purpose, suitability, necessity, free access, data quality, transparency, security, prevention, non-discrimination, and accountability. Additionally, we included some dimensions of software engineering, such as software, research and study, governance, public management, and infrastructure.

We followed the same steps proposed by Sangaroonsilp et al. [32] to develop our taxonomy, which consists of three main steps:

TP1 **Identification of Privacy Requirements**: an analysis of legislation and the framework in search of privacy requirements for the composition of the taxonomy. This step involves a critical analysis of the documents for item composition.
TP2 **Classification of Privacy Requirements**: development of the classification of requirements grouped into categories based on a list of privacy objectives.
TP3 **Refinement of Privacy Requirements**: removal of possible duplicates and adjustment of any inconsistencies considering the existence of two sources for the requirements.

3.3. Taxonomy application

To assess the adequacy of the taxonomy of privacy requirements developed in this work, we undertook a validation process focusing on Open Banking Brasil—a project initiated by the Central Bank of Brazil (BCB) to enhance competitiveness within the financial system by

fostering collaboration and data sharing among financial institutions. This strategic initiative empowers users, allowing them to share their financial data across institutions based on explicit consent.

Open Banking is governed by Joint Resolution No. 1 of the National Monetary Council and the Central Bank, dated May 4, 2020 [60], with a foundational premise that aligns with the Brazilian General Data Protection Law (LGPD) [7]. The regulatory framework of Open Banking Brasil offers an ideal context for evaluating the applicability and relevance of our taxonomy of privacy requirements.

To execute this validation, we devised the Taxonomy Adherence Assessment Form (TAAF), a comprehensive tool designed to evaluate the adherence of financial institutions' data-sharing processes to LGPD principles. The TAAF, available at Zenodo [61] in *TAAF_application.zip*, was crafted by this research's first and third authors. Privacy requirements were categorized into options such as "Yes", "No", "Partially", "Not assessable", and "Not applicable", providing insights into whether the requirements were implemented by each financial institution based on the collected data.

The application of the TAAF involved a thorough analysis of the privacy policies and Terms and Conditions Documents (T&C) for Open Banking of the three largest banks in Brazil [62]. The real names of the banks are omitted to maintain confidentiality and will be referred to as Bank A, Bank B, and Bank C. The T&C documents, transcribed into English, are accessible on Zenodo [61] in *TAAF_application.zip*.

4. Systematic literature review

This section reveals the materials and findings obtained by completing the three main steps of a systematic literature review according to the guidelines proposed by [56]: planning, conducting, and reporting. Here, we delve into the details of each stage, explaining the careful planning, the actual review process, and the comprehensive reporting. The goal is to offer a clear understanding of the specific activities involved in each phase, enhancing clarity about the systematic literature review's steps and methods.

4.1. Planning

The planning phase consisted of defining the research questions, building the generic and database-specific search strings, defining inclusion and exclusion criteria, and creating a quality assessment checklist.

4.1.1. Research questions

This SLR aims to identify in the literature the works that proposed a taxonomy of privacy requirements by answering the following research questions (RQ):

- RQ.1 What are the existing taxonomies of privacy requirements in the literature?
- RQ.2 Is there any taxonomy of privacy requirements in the literature based on the LGPD and ISO/IEC 29100?

4.1.2. Search string

The digital databases ACMDigitalLibrary, Scopus, and WebofScience were used to collect and analyze studies related to the context of taxonomies and privacy requirements. The search string used was: *"Taxonomy" AND ("Requirements Taxonomy" OR "Privacy Requirement Taxonomy" OR "Privacy Requirement Elicitation" OR "Requirements Gathering")*.

4.1.3. Inclusion and exclusion criteria

Studies selected from the search string were analyzed using the Parsifal[1] tool. Study selection criteria were used to identify primary studies capable of providing direct evidence on the research questions. To reduce the probability of bias, the selection criteria were decided during protocol definition, before the research was carried out. This selection was based on the analysis of the defined selection criteria.

Inclusion criteria were: (IC.1) full-text available in English or Portuguese; (IC.2) it was published from 2003 to 2021; and (IC.3) it proposes, analyzes, or applies taxonomies in the context of privacy requirements.

Regarding the exclusion criteria, the following were defined: (EC.1) it does not meet the inclusion criteria; (EC.2) it does not present sufficiently elaborated information such as not presenting the foundation of the methodologies used, unclear writing, or missing the required structure (introduction, development, results, and conclusion); (EC.3) works that do not allow a reliable data extraction, as they do not present results in a systematic, methodological way, as well as sufficient evidence of the results achieved. These selection criteria were applied to the papers' title, abstract, and metadata information.

4.1.4. Quality assessment

The quality assessment questions, considered critical by [56], were defined considering the adequacy of the research questions in order to minimize biases and maximize the validity of the process. The questions that were used to evaluate the pre-selected are: (QA1.) Are aspects related to eliciting privacy requirements addressed in the study? (QA2.) Is the proposed taxonomy related to privacy requirements? (QA3.) Do the authors present the methodology for creating the taxonomy?; and (QA4.) Does the study present the results of the applicability of the methods? For QA2, the following topics were considered as well: security context, regulatory context (government laws), and concepts of transparency and intervention.

The quality assessment process consisted of assigning a score, among Y(Yes) = 1; P(Partially) = 0.5; and N(No) = 0, that indicated whether the paper met each QA. The cut-off score, which works must be equal to or greater than it to be accepted, is a simple average of the sum of scores obtained by each work in each question.

4.2. Conducting

The application of the search string in the three digital databases resulted in 110 papers. The result of this phase is available in the reproduction package available at Zenodo [61] in the *SLR_bibs.zip* file. We removed 15 articles due to duplication. The Scopus database was the one that presented the most duplicated works in relation to the other databases (12 duplicated works). Then, the candidate works were selected considering the inclusion and exclusion criteria. As a result, 74 works were rejected, resulting in 21 works for the quality assessment phase.

By applying quality criteria, only one work obtained a maximum score in the process, three works scored 3.0, one work scored 2.0 (half of the maximum possible), four works scored 1.5, three works scored 1.0, four scored 0.5 points, and two works did not score. Considering the total number of works (21) and the sum of the grades in points (29.5), the average obtained was 1.40. As the score assigned to the QA responses is either 1, 0.5, or 0, the cut-off was rounded to 1.5. Table 1 lists the scores of each paper and presents the selected papers at this step of the protocol.

After conducting the quality assessment phase, we read the full text of the remaining 10 works to identify and confirm their relationship to the context of privacy requirements. During this last process, four papers were removed because they were not related to this SLR context (S5, S7, S9, and S10 from Table 1). The SLR procedure and remaining papers after each step are presented in Fig. 2.

After a complete and full-text read of the selected papers, we discarded some studies that did not approach our subject of interest. More specifically, these works do not present a taxonomy of privacy requirements. This could have happened for a number of reasons such

[1] https://parsif.al/

Table 1
List of selected and removed studies after the application of the quality assessment.

	ID	Author	Year	QA1	QA2	QA3	QA4	*Score*
Selected	S1	Antón and Earp [52]	2004	Y	Y	Y	Y	4.0
	S2	Meis and Heisel [63]	2016	P	P	Y	Y	3.0
	S3	Hernández et al [64]	2010	P	P	Y	Y	3.0
	S4	Meis and Heisel [65]	2017	P	P	Y	Y	3.0
	S5	Siegfried et al. [66]	2020	N	N	Y	Y	2.0
	S6	Rjaibi and Rabai [54]	2015	P	P	P	N	1.5
	S7	Lehnert [67]	2011	Y	P	N	N	1.5
	S8	Bolchini et al. [68]	2003	N	N	P	Y	1.5
	S9	Alhirabi et al. [69]	2021	Y	N	N	P	1.5
	S10	Tang et al. [70]	2021	Y	N	N	Y	1.5
Removed	S11	Azad and Martens [71]	2021	N	N	Y	N	1.0
	S12	Lauenroth et al. [72]	2017	N	N	N	Y	1.0
	S13	Bhatia et al. [73]	2016	P	N	N	P	1.0
	S14	Gómez Sotelo et al. [9]	2018	N	N	P	N	1.0
	S15	Zafar et al. [74]	2020	N	N	P	N	0.5
	S16	Ahmed et al. [75]	2019	N	N	P	N	0.5
	S17	Belani [76]	2012	N	N	P	N	0.5
	S18	Abdelmaboud [77]	2021	N	N	P	N	0.5
	S19	Gordieiev and Kharchenko [78]	2020	N	N	N	P	0.5
	S20	Chen and Dong [79]	2013	N	N	N	N	0.0
	S21	MacRuairi et al. [80]	2008	N	N	N	N	0.0

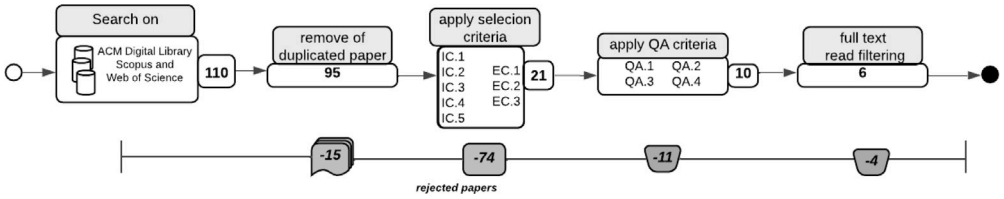


Fig. 2. Number of removed papers at each step of the SLR procedure.

as embracing criteria problems and indexing research problems. Below, we present the reasons for discarding these studies.

Siegfried et al. [66] (S5) provided a taxonomy of system requirements in the Internet of Things Industry (IoT) context. The authors structured system requirements for applications and mapped these requirements to the Blockchain technological idiosyncrasies. The taxonomy was built from an iterative process based on a descriptive literature review. A theoretical application was performed in order to validate the applicability of Blockchain technology to IoT. Therefore, this taxonomy is not related to privacy requirements.

Lehnert [67] (S7) proposed a taxonomy for software impact analysis based on a literature review carried out on studies related to the context of software changes. It was not identified any specific method to elaborate the taxonomy. The authors proposed their own method for correlating the taxonomies found in the literature with the key requirements. They also defined nine key requirements and used the taxonomy to classify five different approaches for impact analysis, demonstrating their applicability. Since this taxonomy is not directly related to requirements but software changes, it was not considered significant for this SLR.

Alhirabi et al. [69] (S9) performed an SLR to address privacy in the realm of IoT in order to analyze techniques, methods and tools to support the requirements of security and privacy in existing non-IoT application designs, enabling their use and integration with IoT applications. The main scope of the article is related to design notations of software, models, and languages that aim to reduce the capture mishaps of non-functional requirements, especially security and privacy requirements. The methodology was an SLR with the Snowballing method that identified 47 notations, languages, and representations for review and comparison. The authors discussed which methods widely adopted, such as STRIDE and LINDDUN, can be adapted for IoT environments, and recorded potential risk management methodologies that can be adapted, such as the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) methodology. The authors registered that the study demonstrated that, although most of the publications analyzed support security requirements in some way, they almost never support data privacy. Although the authors indicate among the main contributions the proposition of a taxonomy, there is no indication of taxonomy in the development or completion of the work, making it unsuitable for this SLR.

Tang et al. [70] (S10) address data privacy in the context of information technology by studying how teams of undergraduates employed privacy idea cards in software development projects. The purpose of using cards is to make privacy concepts more accessible to developers. The authors identified that using the cards promoted a greater understanding of privacy regulations. According to this work, the results indicated that the card application should take into account some intersecting factors, such as the stage at which the cards are used and the autonomy assigned to developers. In the field of teaching, ideation cards have been shown to facilitate low-level cognitive engagement for specific components within a project. This project briefly discussed some privacy concerns but did not present a proposition of taxonomy or any requirement relation, which is not suitable for this SLR protocol.

4.3. Reporting

After meticulously filtering the studies, selected studies underwent a thorough analysis aimed at providing comprehensive answers to the research questions posed. The subsequent section elucidates the responses to these questions.

4.3.1. RQ.1. What are the existing taxonomies of privacy requirements in the literature?

The taxonomies analyzed in this SLR with their respective details are presented in Figs. 3 and 4. Following we detail each one.

The primary study by [52] (S1) proposed a taxonomy of privacy requirements based on website policies in order to mitigate the vulnerability of these websites. The authors used goal mining and goal

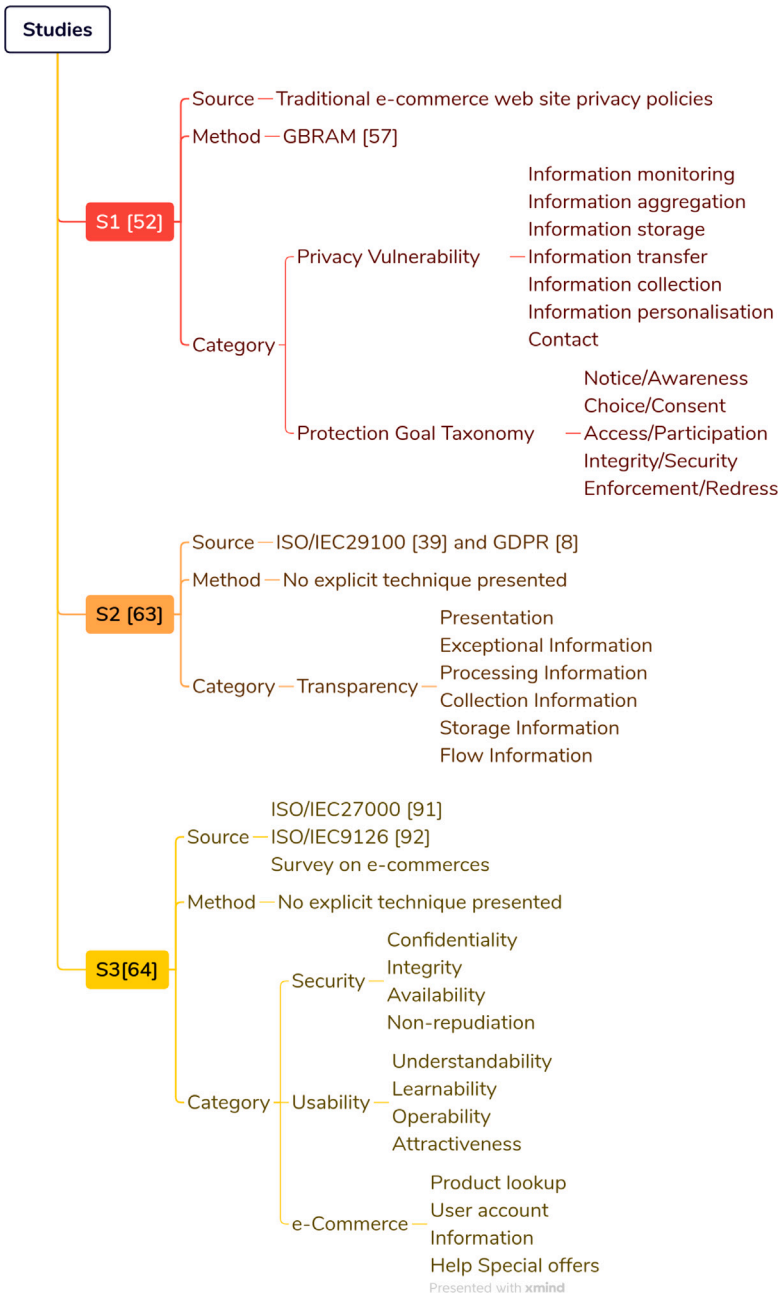


Fig. 3. Taxonomies identified in the SLR — Part 1.
Source: Authors.

extraction from text artifacts prerequisites (site standards). In addition, the authors analyzed an initial set of Internet privacy policies to develop the taxonomy. The taxonomy validation was performed by extracting the goals that involved the privacy policies of some health-related websites. Based on the validation results, the taxonomy was refined, resulting in two classes of privacy requirements: protection goals and vulnerabilities. Protection goals were used to address the desired protection of consumer privacy rights, while vulnerabilities describe requirements that would potentially threaten consumer privacy. This taxonomy scope is websites and it is noteworthy that, as it was previously developed, the implementation of the GDPR can be considered outdated.

The primary study developed by [63] (S2) addressed the importance of privacy as a quality parameter in software development. The authors specifically addressed a privacy objective regarding the empowerment of end-users and how they control the processing of their personal data by information systems. This privacy objective is referred to as intervenability. The authors conducted a survey with end users and found out a lack of intervention options in information systems. They also refined the intervenability objective into a software requirements taxonomy and related them to a transparency requirements taxonomy, because, according to the authors, transparency can be considered a prerequisite for intervention. The purpose of the combined intervenability and transparency requirements taxonomy is to guide requirements engineers in identifying the intervenability requirements relevant to the system. The authors used the ISO/IEC 29100 and the draft of the GDPR to build their taxonomy. The taxonomy was validated in relation to the completeness the requirements by comparing it with some studies recovered by executing a SLR. Intervenability is similar to privacy requirements, however, this work did not show the practical applicability of the taxonomy, and no validation was carried out in a real context.

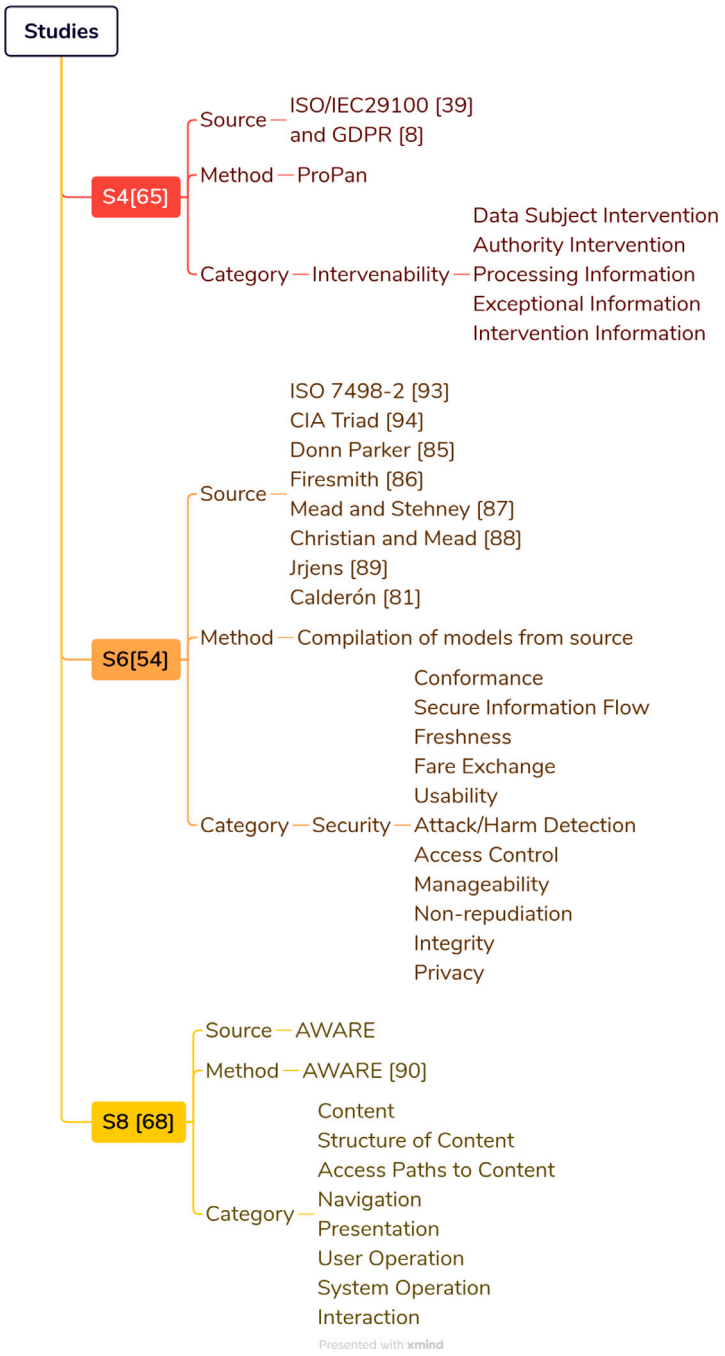


Fig. 4. Taxonomies identified in the SLR — Part 2.
Source: Authors.

Hernández et al. [64] (S3) proposed a taxonomy of requirements composed of security factors, usability, and characteristics for the development of B2C and C2C e-commerce sites. Their work was based on Calderón [81] who proposed a taxonomy of security requirements divided into confidentiality, integrity, availability, and non-repudiation of requirements. For the usability factor, Hernández et al. relied on [82–84] who also divided the attributes of this factor into requirements. Hernández et al. also collected requirements for the e-commerce factor through a survey with users from large sites in the field. As a result, the authors developed a model composed of a formula and a technique to assess the conformity of the functionalities of a B2C or C2C website with regard to the requirements proposed in the requirements taxonomy. The technique used for the validation consisted on the following steps: define a goal; establish constructors to be evaluated; define questions to identify how to measure the attributes; verify the percentage of conformity between the functionalities of a system and its requirements; and obtain the system rate. This taxonomy is not directly related to privacy but to security, in which privacy is included [41,47–49].

Meis and Heisel [65] (S4) is a continuation of the work started in [63] (S2) on intervenability requirements. The main difference from the previous work is the use of the published version of the GDPR on the creation of the taxonomy. In addition, the authors proposed a method called ProPAn for analyzing privacy-based problems. In this method, intervenability and transparency requirements can be generated automatically based on artifacts provided by the ProPAn method and rules derived from GDPR. Furthermore, the method provides requirements validation conditions that can be used to automatically verify user

adjustments to specifications to ensure compliance with the implied needs of the GDPR. The steps of the method are integrated into the ProPAn tool that is automatically executed during the generation and validation. Despite being called a taxonomy of intervenability and transparency, the study has some subjective relationship with privacy requirements.

Rjaibi and Rabai [54] (S6) proposed a security taxonomy with a holistic view based on existing taxonomies in the literature. Safety standards were also considered, such as ISO 7498-2:1989, CIA Triad, Donn Parker, and academic works as well [81,85–89]. The work discussed each of the sources for the taxonomy and presented a comparison between the placement of safety factors in each of the taxonomies. The authors did not present an application of the taxonomy in a real scenario. Furthermore, privacy was addressed as a safety factor in this taxonomy.

Bolchini et al. [68] (S8) proposed a taxonomy for classifying hypermedia requirements. The proposed model adopted an objective-oriented approach along with scenario-based techniques, introducing the hypermedia requirements taxonomy to facilitate the conceptual design of the Web. Bolchini et al.'s taxonomy was based on the AWARE model, which is a specialization of the *i** framework. The taxonomy is composed of eight main categories, and the authors empirically validated the model based on the theory of perceived quality attributes. In addition, a case study was developed for practical validation with industrial partners who demonstrated, in general, that AWARE [90] is a good quality proposal for the requirements of modeling web applications. Despite being a taxonomy of requirements, this proposal did not address the privacy context, focusing only on addressing functional requirements for web applications.

As conclusion to the analysis above, the taxonomies in this SLR were all only partially related to privacy requirements. As summarizing their respective details are presented in Figs. 3 and 4. The Figure has the **S1, S2, S3, S4, S6, and S8** - primary studies identifier; **Source** - source from which the taxonomy requirements were inspired; **Method** - the method used to elaborate the taxonomy; and **Category** - the first level of the requirements category obtained from the taxonomies.

4.3.2. RQ.2. Is there any taxonomy of privacy requirements in the literature based on the LGPD and ISO/IEC 29100?

The SLR did not identify a taxonomy of privacy requirements in the context of LGPD and ISO/IEC 29100. However, it revealed taxonomies that have some relationship with privacy requirements [52,54,63–65,68]. These studies approached the topic indirectly or only through perspectives. Thus, the results of RQ.1 and RQ.2 demonstrate a gap in the literature regarding privacy requirements, especially in the context of personal data protection legislation.

5. Taxonomy proposal

5.1. TP1 - identification of privacy requirements

In this step, the LGPD and ISO/IEC 29100 were analyzed in order to identify statements related to data processing and personal rights. To this end, all LGPD articles were analyzed in which we found statements in 28 articles. Similarly, ISO/IEC 29100 and its 58 statements were analyzed within the privacy principles established by this standard. As a result, we identified 112 privacy requirements from the LGPD and 57 privacy requirements from ISO/IEC 29100. The identification was primarily done by the first author and revised by the second author, during the course of seven months. In case of disagreement, there the authors discussed until they reach a consensus. The details of this process are presented following.

Table 2
Example of applying TP1's steps.

Step	Result
TP1.a	The action required in this declaration is the **indication** by the controller, the action verb used will then be **INDICATE**
TP1.b	The person involved in this declaration is the **controller**, which is the actor who has an obligation
TP1.c	It is verified that the purpose of the declaration is to **indicate the person in charge of processing personal data**
TP1.d	The resulting requirement is *RLGPD069 - INDICATE the person in charge of processing personal data*

TP1.a **Identification of actions:** The statements were evaluated in order to identify those related to actions executed by data processing agents, in order to guarantee data subjects' rights. We also analyzed the declarations from the perspective of data subjects to identify their rights. This analysis aimed to identify actions that refer to requirements that demand implementation by the systems, whether to meet the obligations of treatment agents or to contemplate the rights of data subjects. The question asked by the authors to identify the statements was: "What action should be taken based on this statement?".

TP1.b **Determination of involved/affected parties:** After identifying actions, the next step was to analyze and extract the objects of the actions, which can be absent in some actions. With this, the identification of those responsible for the execution of the actions was carried out. The question that represents this need is "Who is involved/affected by this statement?"

TP1.c **Expected result weighting:** This step aimed to analyze the statements found in the taxonomic base to assess their adherence to the expected result in relation to user privacy. The question that was used to conduct this step was "What should be achieved based on the action of this declaration?".

TP1.d **Structuring into a requirement pattern:** The resulting privacy requirements were structured in the form of <action verb - object - object complement>. Although the authors in [32] do not present the motivation for choosing the word class "verb" to start structuring the requirements, we understood that in the context of taxonomy, action verbs can directly contribute to the clarification of the requirements because they indicate actions to be performed. According to [91], the verb is the key piece in the enunciation of different legal concepts, which supports the structuring starting with this verbal class.

As an example of applying step TP1, consider the following article from the LGPD: *"Art. 41. The controller shall indicate a data protection officer"*.. Now, by applying TP1, we have the results presented in Table 2 and Fig. 5.

5.2. TP2 - classification of privacy requirements

This step defined the taxonomy categories and how the 169 requirements obtained during TP1 execution were classified. Requirements were grouped based on their goals, by executing a process divided into two parts:

TP2.a **Definition of achievements for each privacy goal:** Goals are defined based on what is expected for each principle of the LGPD. This definition was used to identify and gather privacy requirements that have the same purpose as the provisions of a category. This step was be performed only once.

TP2.b **Consideration of the expected result for a requirement:** Classification of the privacy requirements according to the goal for which they are best suited.

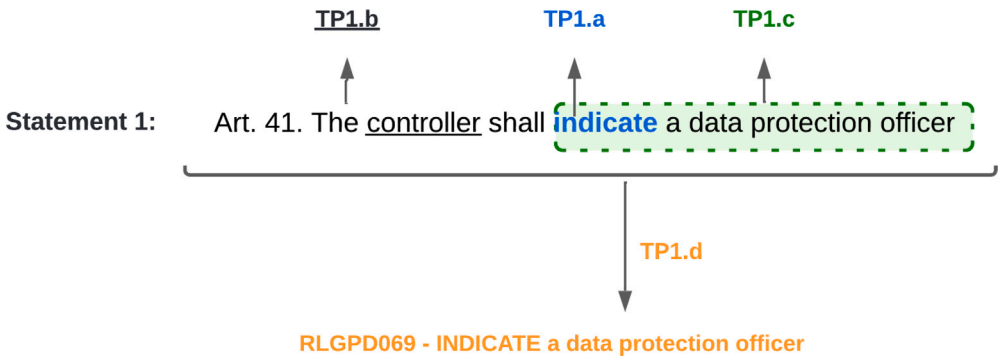


Fig. 5. TP1 - Privacy requirements identification process.
Source: Authors.

For the execution of TP2.a, we considered the principles defined in the LGPD and ISO/IEC 29100. The LGPD has in its composition ten principles that govern the processing of personal data. ISO/IEC 29100, in turn, has nine principles for the implementation and development of Information and Communication Technology systems. The principles of the LGPD and ISO/IEC 29000 share many similarities, as shown in Table 3. Because they are comprehensive, these principles can be used as objective categories for classifying privacy requirements.

It was necessary to create an additional classification for the requirements since the LGPD [7] covers several areas of software engineering and the principles were not enough to classify requirements. Therefore, we defined new contexts to help refine the classification of requirements and help systems analysts identify needs within their organizations. The contexts are presented following.

- C.1 **Software**: requirements that can be implemented in software, that is, system requirements that can be validated by business rules;
- C.2 **Studies and Research**: requirements that determine how research bodies should proceed with the treatment of personal data since it could occur without consent;
- C.3 **Governance**: requirements that cannot necessarily be met by systems, but that need to be implemented by the organization, in which there may be controls and governance mechanisms to guarantee the principles of the LGPD;
- C.4 **Public Management**: requirements that are mandatory for organizations of a public nature, but that need to be implemented by the organization to ensure compliance with legislation regarding data sharing, mainly without the need for consent protected by the right of its nature;
- C.5 **Infrastructure**: requirements on the process of sharing information internationally, transferring data with third parties, and data storage processes and controls.

Privacy requirements can be placed under a category and also be considering in a specific context, which can repeated across different categories. However, a requirement cannot belong to more than one category to avoid redundancy. The category remains the main grouping, as it reflects the principles of the LGPD. Fig. 6 presents the relationships between the categories and contexts.

5.3. TP3 - refinement of privacy requirements

After TP2, we refine the 169 requirements. The refinement process consisted in analyzing the requirements and searching for common ground. This search is better executed after the categorization process, that was performed after TP2. The process of grouping requirements into categories helped on the identification of duplicated requirements which were removed during TP3. We look for possible duplicates requirement as the LGPD, and ISO/IEC 29100 covers much of the same matter, and the taxonomy of [32] found all the ISO/IEC requirements duplicated to the GDPR. We also adjusted some inconsistencies, considering the existence of two sources for the requirements. This was an important step to ensure the integrity and fluidity of the taxonomy.

An example of this execution is the LGPD article "*Art. 8 The consent set forth in item I of article 7 of this Law must be provided in writing or by other means that proves the manifestation of the will of the data subject.*" generated the requirement **RLGPD013 - COLLECT written consent or by another means that demonstrates the holder's expression of will**. Whereas in ISO/IEC 29100 the snippet "*[. . .] obtain the PII principal's optional consent to collect or process confidential PII, except where applicable law permits the processing of confidential PII without the consent of the individual [. . .]*" generated the requirement **RQISO3 - OBTAIN the data subject's optional consent to collect or process the confidential data, except when applicable law allows the processing of confidential data without the consent of the individual**. These two requirements were classified under *P.1 Purpose* category and were merged into a single requirement i.e. **OBTAIN the data subject's optional consent to collect or process confidential data from a stated manifestation of this consent, except where applicable law allows the processing of confidential data without the consent of the individual**.

With the refinement process, 27 requirements were unified with each other, whereas 17 requirements were identified as duplicates. Three requirements obtained from ISO/IEC and three requirements obtained from LGPD were excluded after analysis because they were outside the scope of privacy requirements, resulting in 129 requirements at the end of the process.

5.4. Proposed taxonomy

The proposed taxonomy of privacy requirements is composed of 129 requirements that are divided into ten categories [LP.N] and five contexts [C.N]. The taxonomy with its categories, contexts, and requirements is shown in Fig. 7. The list of privacy requirements generated for this taxonomy is available at Zenodo [61] in *privacy_requirements_taxonomy.pdf*.

Table 4 presents the 18 verbs used by [32] and the 41 verbs used in this work. The verbs common to both processes were highlighted in bold, totaling 14 intersections.

In our work, all of the 65 LGPD articles were analyzed but only 27 articles had statements related to the process of processing personal data and fitted the characteristics highlighted in the steps of the procedure for analysis and design of privacy requirements. The list of select articles are 6–7, 12–25, 29–30, 32–34.

During the execution of the procedure in ISO/IEC 29100, 63 statements were analyzed for the GDPR+ISO/IEC 29100 taxonomy, resulting in 33 requirements, while for the LGPD+ISO/IEC 29100 taxonomy, 58 statements were analyzed, resulting in 57 requirements.

Table 3
Relationship among the principles of LGPD and ISO/IEC 29100.

LGPD	ISO/IEC29100
LP.1 **Purpose**: processing done for legitimate, specific and explicit purposes of which the data subject is informed, with no possibility of subsequent processing that is incompatible with these purposes;	PF.1 **Consent and choice**: enable the data subject to choose the processing of their personal data and provide clear information about the process. It must allow the data subject to decide not to accept the processing of his personal data; PF.2 **Purpose legitimacy and specification**: ensure compliance with the purpose, notifying the user when using the data for a new purpose. Ensure that the information is clear and objective;
LP.2 **Suitability**: compatibility of the processing with the purposes communicated to the data subject, in accordance to the context of the processing;	PF.3 **Collection limitation**: ensure that the personal data collected are only those strictly necessary for the processing of data necessary for the proposed purpose, in addition to being in accordance with existing legislation;
LP.3 **Necessity**: limitation of the processing to the minimum necessary to achieve its purposes, covering data that are relevant, proportional, and non-excessive in relation to the purposes of the data processing;	PF.4 **Data minimization**: it is closely linked to the principle of limitation of data collection, going beyond this principle as it is not only related to the collection but also to the processing of personal data. This is done by minimizing those involved in the treatment, using whenever possible solutions that excel in non-identification; PF.5 **Use, retention and disclosure limitation**: limit the use, retention, and disclosure of personal data to the fulfillment of their purposes and retain personal data only for the time necessary for the purpose for which such data were obtained, applying anonymization processes or securely destroying them;
LP.4 **Free Access**: guarantee to the data subjects of facilitated and free-of-charge consultation about the form and duration of the processing, as well as about the integrity of their personal data;	PF.8 **Individual participation and access**: provide the data subject with means to access and review their personal data, provided that access is authenticated with an appropriate level of security. In addition, establish procedures for holders to exercise their rights;
LP.5 **Data Quality**: guarantee to the data subjects of the accuracy, clarity, relevancy, and updating of the data, in accordance with the need and for achieving the purpose of the processing;	PF.6 **Accuracy and quality**: ensure that personal data is accurate in terms of its origin and collection and that it is always up to date, ensuring its reliability. Ensure that the changes requested by the holder are legitimate and accurate. Propose processes to ensure the accuracy of data collected and processed.
LP.6 **Transparency**: guarantee to the data subjects of clear, precise, and easily accessible information about the carrying out of the processing and the respective processing agents, subject to commercial and industrial secrecy;	PF.7 **Openness, transparency, and notice**: make accessible the information about the processing of personal data. Notify the data subject about the controller and processing information, especially in the event of major changes in the data processing process;
LP.7 **Security**: use of technical and administrative measures which are able to protect personal data from unauthorized accesses and accidental or unlawful situations of destruction, loss, alteration, communication or dissemination;	PF.10 **Information security**: protect data at the necessary levels of controls in operational, functional and strategic procedures in order to guarantee the integrity, confidentiality, and availability of personal data;
LP.8 **Prevention**: adoption of measures to prevent the occurrence of damages due to the processing of personal data;	PF.11 **Privacy compliance**: evaluate and demonstrate that the data processing process complies with the necessary requirements for its protection. Have internal controls adhering to the necessary protection and have external evaluation mechanisms to guarantee the fairness of the process.
LP.9 **Non-Discrimination**: the impossibility of carrying out the processing for unlawful or abusive discriminatory purposes;	
LP.10 **Accountability**: demonstration, by the data processing agent, of the adoption of measures that are efficient and capable of proving compliance with the rules of personal data protection, including the efficacy of such measures	PF.9 **Accountability**: record all procedures, controls, tools, and methods used in data processing, provide adequate training to those involved in the processing of personal data, consider compensation procedures when reversible situations occur, not allowing the holder to return to the initial privacy status;

Whereas [32] identified 33 ISO requirements, our work identified 57. Initially, Sangaroonsilp et al. [32] identified 63 statements from the ISO/IEC 29100 privacy framework. After encoding by three experts, they identified 36 requirements from ISO/IEC 29100. In a subsequent analysis, the authors refined this list to 33 requirements from ISO/IEC 29100. For instance, Sangaroonsilp et al. [32] identified 9 requirements of the "ALLOW" type, while in our research, we identified 7. The complete list of 57 privacy requirements from ISO/IEC 29100 identified in this study versus the requirements identified by Sangaroonsilp et al. is presented on Zenodo [61].

In the refinement process, GDPR+ISO/IEC 29100 unified 78 requirements considered to be similar or duplicated while LGPD+ISO/IEC 29100 performed the unification process for 44 requirements that were duplicated. Despite the GDPR establishing the parameters for the processing of data by public entities, [32] state that none of the requirements reflect public entities whereas, our taxonomy has 11

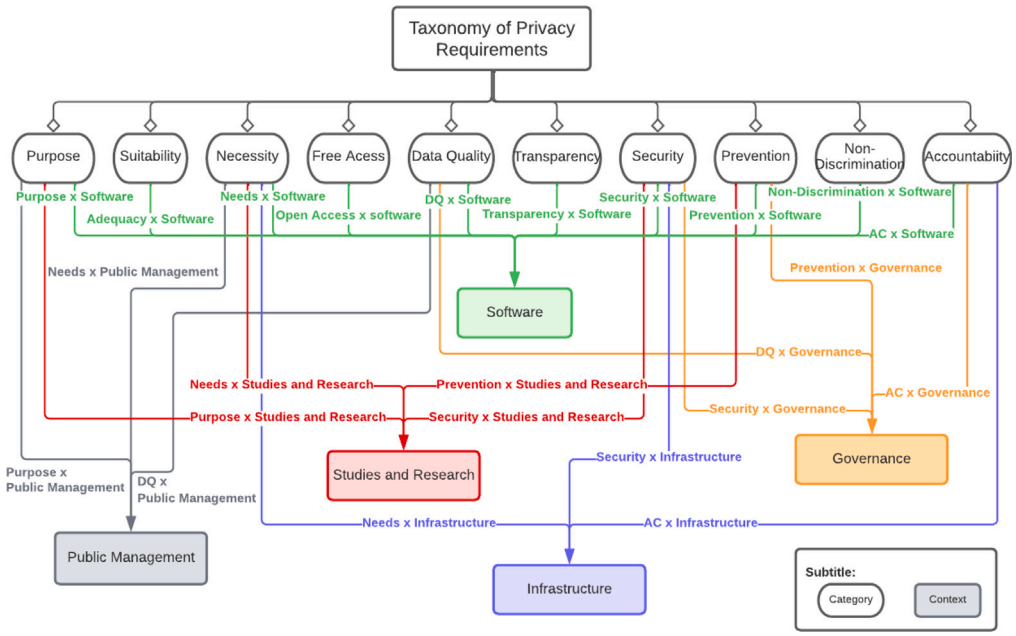


Fig. 6. Structuring of the taxonomy of privacy requirements.

Table 4
Verbs used in our taxonomy compared to those used by [32].

GPDR+ISO/IEC 29100	LGPD+ISO/IEC 29100
Allow, archive, **collect**, **ensure**, **erase**, **implement**, **inform**, **maintain**, **notify**, **obtain**, **present**, **protect**, **provide**, request, show, **store**, transmit, **use**.	Adopt, **allow**, assign, attend, block, **collect**, communicate, consider, delete, develop, discover, document, **ensure**, **erase**, establish, finish, get, guarantee, have, **implement**, indicate, **inform**, keep, limit, **maintain**, make, **notify**, **obtain**, **present**, prevent, prohibit, **protect**, **provide**, publish, resolve, select, **store**, submit, **use**, verify, waive.

Table 5
Comparison between our and [32]'s taxonomies, respectively LGPD+ ISO/IEC 29100 and GPDR+ ISO/IEC 29100.

	LGPD+ ISO/IEC 29100	GPDR+ ISO/IEC 29100
TP1		
Analyzed studies	27	18
Analyzed ISO/IEC statements	58	63
Requirements extracted from the law	112	116
Requirements extracted from the ISO/IEC	57	33
TP2		
Categories	10	7
TP3		
Verbs used	41	18
Final number of requirements	129	71

requirements that are directly related to the processing of data by legal entities of a public nature.

Regarding the contexts of the present taxonomy, five requirements are related to handling data for Research and Study purposes, 26 requirements are related to the governance of institutions, nine privacy requirements related to infrastructure solutions, and one related to health. The number of requirements generated by the taxonomies also differs since the GDPR+ISO/IEC 29100 taxonomy is composed by 71 requirements and the LGPD+ISO/IEC 29100 taxonomy has 129 privacy requirements, as seen in Table 5.

Notable differences between this taxonomy and Sangaroonsilp et al. include two requirements in the "Purpose" category. In the context of "Study and Research", RQ019 aims to enable the preservation of personal data after the completion of its processing, specifically for studies conducted by research entities. This aligns with Article 16 of the LGPD, which mandates the elimination of personal data after processing, with the exception that research entities, whether public or private, can retain data for study purposes, provided anonymization is ensured whenever possible.

In the realm of "Public Management", RQ021 involves informing data subjects that the right to request information can also be exercised with consumer protection agencies. Article 18 of the LGPD grants citizens this right, allowing them to seek information about the use of their personal data from any public entity, whether municipal, state, or federal.

In the "Accountability and Reporting" category, especially in the context of "Governance", Article 49 of the LGPD requires that software systems used for personal data processing be structured to meet security requirements, good practice standards, governance, and general principles outlined in the LGPD, as well as other regulatory standards. In this context, the proposed taxonomy introduces RQ121, highlighting the need to implement these requirements in systems used for personal data processing, ensuring compliance with legal requirements.

Regarding requirements identified from ISO/IEC 29100, we emphasize two: RQISO22, which underscores the need to ensure that processed information is accurate, complete, and up-to-date, unless there is a legitimate basis to maintain outdated data; and RQISO24, which addresses the proper verification of the validity and accuracy of claims made by the information controller before making any changes, ensuring that such changes are duly authorized when appropriate. Notably, these requirements were not identified by Sangaroonsilp et al.

6. Taxonomy application

The TAAF application for Bank A on relation to the Open Banking project identified that 24.81% of requirements were implemented (yes), 2.33% not implemented (no), 13.18% were marked as partially applied, 19.38% did not relate to the context of FIs, and 40.31% of the requirements could not be evaluated with the available information. Analyzing the results, discarding not assessable or non-applicable requirements

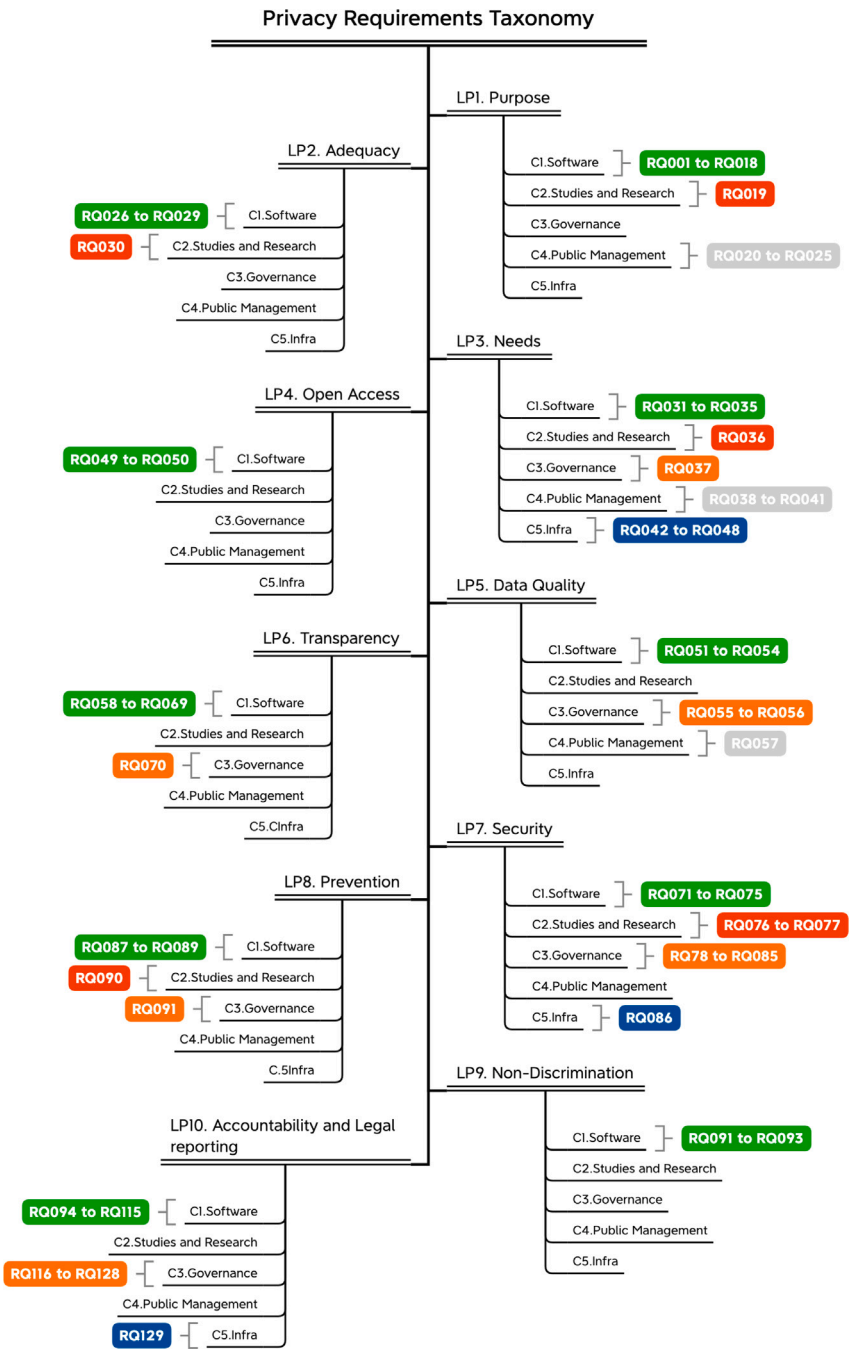


Fig. 7. Privacy requirements taxonomy.

for FIs, it is found that 61.54% of the requirements were identified as applied by Bank A, while 32.69% were considered partially applied and 5.77% were considered not applied.

On relation to Bank B, the TAAF resulted in 28.68% of implemented requirements (yes), 10.85% of the requirements partially implemented, 0.78% of the requirements were not implemented (no), 40.31% were considered non-evaluable with the available information, and 19.38% of the requirements were considered unrelated to the context of financial institutions (not applicable). From the perspective of privacy requirements, removing the requirements identified as not applicable and not assessable, we found out that 71.15% of the privacy requirements were implemented, 26.92% partially applied and only 1.92% were not implemented.

Finally, for Bank C, the application of the TAAF resulted in 16.28% implemented requirements (yes), 2.33% of the requirements were not implemented (no), 21.71% were considered partially implemented, 40.31% were considered non-evaluable with the information available and finally 19.38% of the requirements were considered unrelated to the context of financial institutions (not applicable). Considering only the requirements marked with "yes", "no"and partially", the institution reached the record of 53.85% of the requirements considered partially met, while 40.38% were considered implemented and 5.77% were considered not implemented.

The overview of the result of the institutions' adherence to the taxonomy from the application of the TAAF is presented in Table 6.

The following paragraphs describe the results of the applicability of the requirements according to the categories they fall into.

LP.1 Purpose - This category has 25 requirements distributed in the contexts of Software, Research and Study, and Governance. 16 requirements were identified as non-evaluable or not applicable for all

Table 6
Comparison of results by institution.

Bank	Application of the privacy requirements					
	Yes		Partially		No	
	%	#	%	#	%	#
Bank A	61.54%	32	32.69%	17	5.77%	3
Bank B	71.15%	37	26.92%	14	1.92%	1
Bank C	40.38%	21	53.85%	28	5.77%	3

FIs. For **Bank A**, four requirements (RQ002, RQ09, RQ014 and RQ015) were identified as fully applied for this purpose by this institution, and five requirements were identified as not or partially applied. Requirements RQ001, RQ004, RQ006, and RQ008 were partially applied in the Software context. RQ001 was considered partially applied because the institution does not allow editing the scope of shared data and it only allows two types of sharing terms, **not considering the free and specific form provided for this requirement**. RQ004 had the application considered as partial because there is no determination of the treatment period by the FI, only the sharing period. RQ006, on the other hand, had the application identified as partial, as there was no public page on the procedures for revocation of consent, however, in the T&C, there is a specific section on the revocation process but no determination of the procedures. Lastly, considering RQ008, the purpose is defined as *offering solutions more adhere to your profile in a secure and confidential way*, however, the institution does not allow changing the scope of shared data.

In the context of Public Management, we found out that RQ021 was not implemented because it was not possible to identify a statement about the possibility of requesting information from consumer protection bodies in the T&C and on the IF privacy page. For **Bank C**, RQ001 was identified as partially met, as it allows only four types of sharing terms, not considering the **free and specific form of the requirement**.

The RQ002 requirement was identified as partially applied because a text is presented that seems to be the purpose of data processing in the data sharing flow in a subjective way, which can impair the identification by the customer. There is no possibility of choosing between these items and item 7 of the T&C states that the **data will be used for the purposes indicated in the consent**.

Furthermore, requirement RQ004 was considered to have been partially met since there is no stipulation of the treatment period, only the sharing period. Although on its General Terms and Conditions page there is the information **that the period for which Bank C keeps the Personal Data collected depends on the purpose and nature of the data processing**. Requirement RQ006 was also considered partially met, as in its General Terms and Conditions page available in the T&C there is a reference to a privacy page of Bank C that discusses the channel for revocation, but there are no details of the necessary procedures. Requirements RQ008, RQ014, and RQ015 had the status assigned as partially met, due to the purpose being presented subjectively and comprehensively in its presentation to the user. In addition, requirement RQ009 was considered partially met, as the purpose is subjectively presented at the time of sharing, and there is no explicit mention of the purpose provided for in this requirement in the T&C, there is only item 4, the statement **preserves the right to process your data, in line with the limits of the LGPD**.

Finally, for Bank C, RQ021 was considered not implemented as no mention was identified of the possibility of requesting information from consumer protection bodies in the T&C and on the IF privacy page. For **Bank B**, 7 requirements were considered as applied - Yes - which are RQ001, RQ002, RQ006, RQ008, RQ009, RQ014, and RQ015. Requirement RQ004 was considered partially met since there is no stipulation of the treatment period, only the sharing period. RQ021 was considered not implemented, since no mention was identified of the possibility of requesting information by consumer protection bodies in the T&C and on the IF privacy page.

LP.2 Suitability - This category is composed of five requirements divided between the Software and Research and Study contexts. Of these, two requirements, one from each context, were considered not applicable. For Bank A and Bank C, three were considered implemented by all FIs (**Bank A, Bank C, and Bank B**), which are RQ027, RQ028, and RQ029. No requirements were identified as not or partially implemented.

LP.3 Necessity - The category is composed of 18 requirements, divided into five contexts. Of these requirements, nine were considered non-applicable or non-evaluable. For **Bank A** and **Bank B**, no requirements were considered not applied. The requirements RQ031, RQ033, and RQ034, the three from the Software context, were considered applied - Yes - by the IF, and six requirements were considered as partially applied, which will be detailed below. The 6 requirements RQ042, RQ044, RQ045, RQ046, RQ047 and RQ048 in this category, all in the Infrastructure context, were considered to have been partially met, since, for the first bank, the general Privacy Policy page, referenced in the T&C, states that the transfer process is done in accordance with the LGPD but there is no evidence to prove the application. For the second, the provisions on the Privacy Policy page contained in the T&C do not mention the transfer process, which may indicate that the institution does not do so or has not contemplated the situation in its privacy policy. For **Bank C**, 5 were considered to have been partially met, namely RQ042, RQ045, RQ046, RQ047, and RQ048, as in its general Terms and Conditions page available in the T&C there is a reference to the privacy page of IF that discusses the international transfer of data is in accordance with the LGPD, but it is possible to prove it with evidence from the information used in this work. The RQ044 requirement was considered as not implemented because although in its general Terms and Conditions page available in the T&C, there is a reference to the IF privacy page that discusses the international transfer of data being in accordance with the LGPD, however in the T&C the institution does not seem to determine as mandatory the reading of the terms that appear in its general page of Terms and Conditions.

LP.4 Free Access - This category is composed of 2 requirements, both from the Software context. For **Bank A**, **Bank C** and **Bank B**, RQ049 and RQ050 were considered partially met because, despite not being directly available in the consent process, the T&C of the FIs mentions in the Privacy policy page of the first bank that contains a section "Your data, your rights", for the second FI the T&C abstractly mentions the general terms and conditions page that contains a section "Your rights" that explains about the rights and how to exercise them. And for the third bank, despite not being directly available in the consent process, the T&C mentions the Privacy Policy page that contains a "your rights" section regarding data access.

LP.5 Data Quality - The Data Quality category is divided into 3 contexts, which are Software, Governance, and Public Management. 5 requirements were considered non-evaluable, 2 from the Software context, 2 from Governance, and 1 from Public Management. Requirement RQ051 was considered to be applied - Yes - by all FIs **Bank A**, **Bank C**, and **Bank B**. RQ052, from the software context, was considered as partially met, also all FIs **Bank A**, **Bank C** and **Bank B**, because despite not being directly available in the consent process the T&C mentions the Privacy Policy page of the first bank which contains a section "your data, your rights", for the second the T&C mentions in an abstract way the general terms and conditions page of the IF which contains a section "Your rights" that explains about the rights and how to exercise them. And for the third party because, despite not being directly available in the consent process, the T&C mentions the Privacy Policy page, which contains a "your rights" section regarding data access.

LP.6 Transparency - In the Transparency category composed of 13 requirements, divided between the software and governance contexts. 4 requirements, from the software category, were considered non-evaluable or not applicable. No requirements in this category were considered not to be applied by all FIs (**Bank A, Bank C, and Bank B**). For *Bank A*, 8 requirements were considered as applied - Yes -

being them RQ060, RQ061, RQ063, RQ065, RQ066, RQ067, RQ68, and RQ070. And RQ069 was considered partially met because, despite the T&C mentioning the Privacy Policy page that refers to the deletion process, there are not many instructions that allow the user to understand it. For *Bank C*, 4 requirements were considered implemented - Yes - which are RQ061, RQ065, RQ066, and RQ067. While 5 requirements were considered as partially applied, requirements RQ060, RQ063, RQ068, and RQ069 received this status because despite not being directly available in the consent process and there is no mention in the T&C on how to exercise the rights, the T&C abstractly mentions the IF general terms and conditions page which contains a "Your Rights" section that explains the rights and how to exercise them. Requirement RQ070 is also considered partially met, in its T&C it mentions in an abstract way the IF general terms and conditions page, a page in which there is section 10. DATA PROTECTION OFFICER, but there is no indication of the name of the in-charge, just an institutional e-mail to activate it. For **Bank B**, requirements RQ060 and RQ069 were considered partially met. The first is that it is informed on the Privacy Policy page about the possibility of requests, but the 15-day deadline is not provided on this page and there is a prior justification for a possible delay. As for the second requirement, despite the fact that the T&C mentions the Privacy Policy page that refers to the exclusion, there are not many instructions that allow the user to understand it.

LP.7 Security - This category comprises 16 requirements distributed among the Software, Research, and Study, Governance and Infrastructure contexts. Of these, 15 requirements were considered non-applicable or non-evaluable. RQ084 was considered as partially serviced by all FIs (**Bank A, Bank C, and Bank B**), as some controls are registered by the banks on their respective privacy sites, but it is not possible to evaluate only with the public information available whether the applicability of the requirement is complete.

LP.8 Prevention - The Prevention category is composed of 5 requirements divided between the Software, Research and Study, and Governance contexts. The 5 requirements were considered non-evaluable or not applicable.

LP.9 Non-Discrimination - This is the smallest category with only 2 requirements in the Software context, both of which were considered not applicable or not assessable. No requirements were considered to be applied, not applied, or partially applied by the FIs.

LP.10 Accountability - This category is composed of 36 requirements distributed among the Software, Governance, and Infrastructure contexts. 19 requirements were considered non-evaluable while no requirements were considered non-applicable. For **Bank A**, 13 requirements from the Software and Governance contexts were considered as applied by the FI - Yes -, which are RQ102, RQ103, RQ105, RQ106, RQ107, RQ108, RQ109, RQ110, RQ112, RQ113, RQ115, RQ116 and RQ123. 2 requirements were considered not applied and 2 were considered partially applied. The requirements RQ094 and RQ104 were considered not implemented - No - because during the analysis no section on the types of personal data collected was identified on the Privacy Policy page to which the T&C refers. Requirement RQ111 was considered partially met because no section on anonymization was identified. While for RQ129 the partial status was assigned because the guarantee of its application is not assessable, however, the FI declares that it follows the procedures, as provided on the Privacy Policy page. For **Bank C**, 10 requirements of the Software and Governance context were considered applied - Yes -, which are RQ102, RQ103, RQ109, RQ110, RQ112, RQ113, RQ115, RQ116 and RQ123. The requirements RQ104, RQ105, RQ106, RQ107, and RQ108 were considered to be partially met because there is mention of anonymization, blocking, or elimination of unnecessary, excessive, or non-conforming data, but there is no explanation of the procedures in its general terms and conditions page. While RQ129, also partially attended, differs in its assessment, as the guarantee is not assessable, but the FI declares that it follows the procedures on the general terms and conditions page. Also for **Bank C**, the RQ094 requirement was considered as not implemented due to the lack of a section on the types of personal data collected in the FI's general terms and conditions pages available in the T&C and on the IF Privacy Policy. Finally, **Bank B** had 16 requirements considered to be applied - Yes -, which are RQ094, RQ102, RQ103, RQ104, RQ105, RQ106, RQ107, RQ108, RQ109, RQ110, RQ112, RQ113, RQ115, RQ116, and RQ123. The RQ129 requirement was considered partially met, as the guarantee is not available, but the IF declares that it follows the procedures on its Privacy page.

7. Discussion

Based on a global analysis of the results, the category with the highest percentage of adequacy was *Accountability*, which reached 25% adequacy in relation to the total number of requirements. This may have happened because this category contains the highest number of evaluated requirements (represents 32.69%), and Bank B was the one with the highest adherence in this category. This percentage of adherence may be due to the fact that this category is related to the external activities that the organization needs to perform to demonstrate adherence to the LGPD, such as the requirements from RQ102 to RQ108, which establish the need to publish necessary procedures for the user to exercise their rights.

Previous work carried out from the perspective of employees indicated that institutions were still starting to apply the LGPD [6]. However, the results obtained in this work indicate greater adherence of the Open Banking project to the proposed taxonomy of privacy requirements, which may have happened because this project was defined after the publication of the LGPD and during its entry into force (2020), in addition to being a project regulated by the Central Bank, an institution with supervisory power [60].

From an academic point of view, we can consider that the finding of this SLR presents a scenario where there is a gap regarding privacy requirements. Although privacy laws across share many similarities, they have peculiarities that require specific tools to help reach full compliance. In this sense, this taxonomy can support this gap for software development and data treatment that is being conducted within the Brazilian territory, which must comply with the LGPD. More broadly, the taxonomy can be used as a reference for the development of other taxonomies that intend to address other privacy laws around the world.

As a practical implication, we were able to cross the academic barrier and verify that there is low compliance in a real-world application since we evaluated three Brazilian banks with a strong presence in the market. This result is a strong indicator that big companies have a long way to go to be fully LGPD compliant, and smaller organizations probably need even more. We believe that the taxonomy can contribute to the industry as a way to verify compliance with the LGPD in their implemented systems, as shown by our use case with Brazilian banks.

However, one practical limitation is that laws are subject to change. The first and worst alternative to deal with the change would be to redo the process. However, the best strategy would be to trace back the requirements and identify the article that has changed. After tracking backward and identifying the article, it would only be necessary to do the forward process again and make changes only to it and not to the entire taxonomy.

8. Threats to validity

The approach proposed by [92] was used to identify the threats to the validity of this study. It is understood that conclusions about the theory defined in the hypotheses are drawn from the observations generated. When drawing conclusions, there are four stages, in each of which there is a type of threat to the validity of the results that are presented below.

Construction validity. The quality of the procedures established for the validation of the work is fundamental for its result. In this sense,

the definition of the taxonomy application evaluation form excelled in the establishment of objective questions built from the proposed taxonomy (cause). Threats may be related to the reduced research population for applying the taxonomy, however, the research population was selected from the impact on the financial market in relation to the size of institutions and how they reflect a considerable portion of this marked in the Brazilian scenario. As a form of mitigation, the concern with the reproduction of the study was also considered to confirm the results in future works and allow new analyzes from different perspectives.

Internal validity. The selection of objects of study may have interfered with the internal validity of this work since it only considered the size of the institution. This criterion was intended to delimit a sample of the financial market, without proposing any pre-deletion in relation to the selected institutions. Regarding the proposal of the taxonomy, it is not possible to rule out bias and legal inconsistencies, but we adopted some measures to mitigate it: the first three authors took a training course on the LGPD; the results of each step was reviewed by at least one author; and we have retained the letter of the law wherever possible and, when amended, we have carefully selected words that retain the original meaning.

External validity. Although this research cannot be considered as capable of covering the Brazilian industrial financial scenario in relation to LGPD, the chosen population covers a considerable part as it includes the 3 largest banks in the country. The intention is not to delimit the LGPD coverage threshold, but to bring evidence that the proposed taxonomy can help development teams in adapting to legislation. Furthermore, a considerable number of requirements were not applicable to the context of financial institutions, either because they were not relevant or due to the limitation of analyzing only privacy policies, which represent the sole publicly available information for analysis. This choice may limit the generalizability of the findings to other contexts where analysis of the productive environment and private documentation is feasible.

Validity of conclusion. The reliability of treatment implementation was a concern in carrying out the research. Regarding the literature review, the number of works identified by the search string was lower than that commonly identified in SLRs, in addition, the lack of adherence of primary works in relation to the scope of research of privacy requirements was also considered a threat. As a minimization strategy, the searches were performed individually in each database, with individualized strings, to ensure that the particularities of their search processes were met. As the application was executed from a subjective analysis performed by two people and not by a machine or a code, there is always the risk of executor bias. As a way of minimizing this threat, the form was made with standardized responses, and justifications for responses with a possible negative impact on the research were added as a way of recording the analyzes assigned during treatment. The minimization of the random heterogeneity of the study population was also considered with the selection of large financial institutions in the country, which allowed the researchers to be analyzed from a homogeneous perspective, providing a good characterization of the analyzed group.

9. Conclusion

In this work, a systematic literature review was conducted, which identified 110 preliminary studies and, after applying the inclusion and exclusion criteria, resulting in the selection of 10 primary studies for data extraction. As a result of the review, it is possible to notice an absence of taxonomies related to the LGPD and ISO/IEC 29100, unveiling a gap in the literature in terms of taxonomies of privacy requirements. In this sense, this work proposed a taxonomy of privacy requirements based on LGPD and ISO/IEC 29100 and the elaboration of the taxonomy used the GBRAM and Ground Theory methods.

The proposed taxonomy resulted in 129 privacy requirements divided into 10 categories (LGPD principles) and 5 application contexts (Software, Research and Study, Governance, Public Management, and Infrastructure) for these requirements. Then, a taxonomy applicability form was developed and applied in a practical case study. The application of the taxonomy occurred from the execution of the application procedures foreseen in the form in the Open Banking project of three financial institutions. The results showed percentages between 40% and 71% of adherence to the evaluated solutions in relation to the taxonomy. This indicates an evolution on the part of institutions in the implementation of privacy requirements in relation to previous research.

The results showed that the taxonomy can be applied in real contexts, allowing the assessment of adherence to Brazilian legislation. In future work, we intend to apply the taxonomy of privacy requirements proposed in this work in a supervised case study with the application in a system under construction with the support of the institution involved in the study so that it is possible to assess the completeness of the privacy requirements of this taxonomy and make adjustments, if necessary.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data is available at https://zenodo.org/doi/10.5281/zenodo.6590218.

Acknowledgments

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

References

[1] P. da República, Lei nº 12.965, marco civil da internet, 2014, URL http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

[2] ANPD, ANPD está apurando no caso do vazamento de dados de mais de 220 milhões de pessoas, 2021, URL https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-esta-apurando-no-caso-do-vazamento-de-dados-de-mais-de-220-milhoes-de-pessoas, (Last access on 16 August 2021).

[3] EBC, Procon de SP notifica empresas de telefonia sobre vazamentos de dados., 2021, URL https://agenciabrasil.ebc.com.br/justica/noticia/2021-02/procon-de-sp-notifica-empresas-de-telefonia-sobre-vazamentos-de-dados, (Last Access on 16 August 2021).

[4] C. Alves, M. Neves, Especificação de requisitos de privacidade em conformidade com a LGPD: Resultados de um Estudo de Caso, in: B. Cruz, A. Hadad, B. Marques (Eds.), Anais do WER21 - Workshop em Engenharia de Requisitos, Editora PUC-Rio, Brasília, DF, 2021, pp. 1–14.

[5] EBC, Sites e aplicativo do Ministério da Saúde sofrem ataque cibernético, 2021, URL https://agenciabrasil.ebc.com.br/saude/noticia/2021-12/sites-e-aplicativo-do-ministerio-da-saude-sofrem-ataque-cibernetico. (Last access on 15 January 2022).

[6] S.E.R. Ferrao, A.P. Carvalho, E.D. Canedo, A.P.B. Mota, P.H.T. Costa, A.J. Cerqueira, Diagnostic of data processing by Brazilian organizations—A low compliance issue, Information 12 (4) (2021) 30, http://dx.doi.org/10.3390/info12040168, URL https://www.mdpi.com/2078-2489/12/4/168.

[7] N.C. da República, Brazilian general data protection law (LGPD), 2018, pp. 1–31, Nartional Congress, accessed in April 10, 2022 1 (1). URL https://www.pnm.adv.br/wp-content/uploads/2018/08/Brazilian-General-Data-Protection-Law.pdf.

[8] E. Parliament, C.o. European Union, General data protection regulation (GDPR), 2016, p. 88, URL https://gdpr-info.eu/, (Last access on 10 April 2022).

[9] K.I. Gómez Sotelo, C. Baron, P. Esteban, C.Y. Estrada, L.d.J. Laredo Velázquez, How to find non-functional requirements in system developments, IFAC-PapersOnLine 51 (11) (2018) 1573–1578, http://dx.doi.org/10.1016/j.ifacol.2018.08.272.

[10] M. Christel, K. Kang, Issues in Requirements Elicitation, Tech. Rep. CMU/SEI-92-TR-012, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, 1992, URL http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=12553.

[11] C.L. Pacheco, I.A. García, M. Reyes, Requirements elicitation techniques: A systematic literature review based on the maturity of the techniques, IET Softw. 12 (4) (2018) 365–378.

[12] W.E. Rzepka, A requirements engineering testbed: Concept, status and first results, in: Proceedings of the Twenty-Second Annual Hawaii International Conference on System Sciences. Volume II: Software Track, Vol. 2, IEEE Computer Society, Kailua-Kona, HI, USA, 1989, pp. 339–340.

[13] W. Behutiye, P. Karhapää, D. Costal, M. Oivo, X. Franch, Non-functional requirements documentation in agile software development: Challenges and solution proposal, in: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 10611 LNCS, (no. December) 2017, pp. 515–522, http://dx.doi.org/10.1007/978-3-319-69926-4_41.

[14] L. Cao, B. Ramesh, Agile requirements engineering practices: An empirical study, IEEE Softw. 25 (1) (2008) 60–67, http://dx.doi.org/10.1109/MS.2008.1.

[15] A. De Lucia, A. Qusef, Requirements engineering in agile software development, J. Emerg. Technol. Web Intell. 2 (3) (2010) 212–220, http://dx.doi.org/10.4304/jetwi.2.3.212-220.

[16] B. Paech, D. Kerlow, Non-functional requirements engineering - quality is essential, in: Proceedings of the 10th International Working Conference on Requirements Engineering: Foundation for Software Quality, REFSQ'04, Springer, Riga, Latvia, 2004, p. 14.

[17] A. Borg, A. Yong, P. Carlshamre, K. Sandahl, The bad conscience of requirements engineering : An investigation in real-world treatment of non-functional requirements, in: Proceedings of the 3rd Conference on Software Engineering Research and Practice in Sweden, SERPS'03, Linköpings universitet, PELAB, Sweden, 2003, p. 8.

[18] D. Ameller, C. Ayala, J. Cabot, X. Franch, How do software architects consider non-functional requirements: An exploratory study, in: 2012 20th IEEE International Requirements Engineering Conference, RE 2012 - Proceedings, IEEE, Chicago, IL, USA, 2012, pp. 41–50, http://dx.doi.org/10.1109/RE.2012.6345838.

[19] J. Eckhardt, A. Vogelsang, D.M. Fernández, Are "non-functional" requirements really non-functional? An investigation of non-functional requirements in practice, in: Proceedings of the 38th International Conference on Software Engineering, ICSE '16, Association for Computing Machinery, New York, NY, USA, 2016, pp. 832–842, http://dx.doi.org/10.1145/2884781.2884788.

[20] R. Berntsson Svensson, T. Gorschek, B. Regnell, Quality requirements in practice: An interview study in requirements engineering for embedded systems, in: Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 5512 LNCS, Springer-Verlag, Berlin, Heidelberg, 2009, pp. 218–232, http://dx.doi.org/10.1007/978-3-642-02050-6_19.

[21] V. Ayala-Rivera, L. Pasquale, The grace period has ended: An approach to operationalize GDPR requirements, in: 2018 IEEE 26th International Requirements Engineering Conference, RE, IEEE Computer Society, Banff, AB, Canada, 2018, pp. 136–146, http://dx.doi.org/10.1109/RE.2018.00023.

[22] E. Dias Canedo, A. Toffano Seidel Calazans, E. Toffano Seidel Masson, P.H. Teixeira Costa, F. Lima, Perceptions of ICT practitioners regarding software privacy, Entropy 22 (4) (2020) 1–23, http://dx.doi.org/10.3390/e22040429, URL https://www.mdpi.com/1099-4300/22/4/429.

[23] M. Maia Peixoto, A Privacy Requirements Specification Method for Agile Software Development Based on Exploratory Studies (Ph.D. thesis), Universidade Federal de Pernambuco, 2021, p. 41, URL http://cin.ufpe.br/~posgraduacao.

[24] P. Anthonysamy, A. Rashid, R. Chitchyan, Privacy requirements: Present & future, in: 39th IEEE/ACM International Conference on Software Engineering: Software Engineering in Society Track, ICSE-SEIS 2017, Bueons Aires, Argentina, May 20-28, 2017, IEEE Computer Society, Bueons Aires, Argentina, 2017, pp. 13–22, http://dx.doi.org/10.1109/ICSE-SEIS.2017.3.

[25] M.T.J. Ansari, A. Baz, H. Alhakami, W. Alhakami, R. Kumar, R.A. Khan, P-STORE: Extension of STORE methodology to elicit privacy requirements, Arab. J. Sci. Eng. 46 (9) (2021) 8287–8310, http://dx.doi.org/10.1007/s13369-021-05476-z.

[26] L. Guzmán, M. Oriol, P. Rodríguez, X. Franch, A. Jedlitschka, M. Oivo, How can quality awareness support rapid software development? - A research preview, in: P. Grünbacher, A. Perini (Eds.), Requirements Engineering: Foundation for Software Quality - 23rd International Working Conference, REFSQ 2017, Essen, Germany, February 27 - March 2, 2017, Proceedings, in: Lecture Notes in Computer Science, vol. 10153, Springer, Cham, 2017, pp. 167–173, http://dx.doi.org/10.1007/978-3-319-54045-0_12.

[27] T. Kanwal, A. Anjum, A. Khan, Privacy preservation in e-health cloud: Taxonomy, privacy requirements, feasibility analysis, and opportunities, Clust. Comput. 24 (1) (2021) 293–317, http://dx.doi.org/10.1007/s10586-020-03106-1.

[28] A.K. Massey, A.I. Antón, A requirements-based comparison of privacy taxonomies, in: First International Workshop on Requirements Engineering and Law, RELAW 2008, Barcelona, Spain, September 9, 2008, IEEE Computer Society, Barcelona, Spain, 2008, pp. 1–5, http://dx.doi.org/10.1109/RELAW.2008.1.

[29] K. Barker, M. Askari, M. Banerjee, K. Ghazinour, B. MacKas, M. Majedi, S. Pun, A. Williams, A data privacy taxonomy, in: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 5588 LNCS, 2009, pp. 42–54, http://dx.doi.org/10.1007/978-3-642-02843-4_7.

[30] R. Meis, R. Wirtz, M. Heisel, A taxonomy of requirements for the privacy goal transparency, in: S. Fischer-Hübner, C. Lambrinoudakis, J. López (Eds.), Trust, Privacy and Security in Digital Business - 12th International Conference, TrustBus 2015, Valencia, Spain, September 1-2, 2015, Proceedings, in: Lecture Notes in Computer Science, vol. 9264, Springer, Cham, 2015, pp. 195–209, http://dx.doi.org/10.1007/978-3-319-22906-5_15.

[31] I. Alqassem, D. Svetinovic, A taxonomy of security and privacy requirements for the internet of things (IoT), in: 2014 IEEE International Conference on Industrial Engineering and Engineering Management, IEEM 2014, Selangor Darul Ehsan, Malaysia, December 9-12, 2014, IEEE, Selangor, Malaysia, Asia, 2014, pp. 1244–1248, http://dx.doi.org/10.1109/IEEM.2014.7058837.

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

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

[34] E.U. Directive, 95/46/EC protection of individuals with regard to the processing of personal data and on the free movement of such data, Offic. J. EC 23 (1995) 31–50, URL https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.

[35] C. Tikkinen-Piri, A. Rohunen, J. Markkula, EU General Data Protection Regulation: Changes and implications for personal data collecting companies, Comput. Law Secur. Rev. 34 (1) (2018) 134–153, http://dx.doi.org/10.1016/j.clsr.2017.05.015.

[36] European Commission, Guidelines on the application and setting of administrative fines, 2021, URL https://ec.europa.eu/newsroom/article29/items/611237. (Last access on 13 October 2021).

[37] UNCTAD, Data protection and privacy legislation worldwide, 2020, URL https://unctad.org/page/data-protection-and-privacy-legislation-worldwide. (Last access on 13 October 2021).

[38] ANPPD, Portal das violações - LGPD, 2021, URL https://anppd.org/violacoes. (Last access on 13 October 2021).

[39] ISO/IEC, ISO/IEC 29100:2011 information technology - security techniques - Privacy framework, 2011.

[40] G. Skinner, S. Han, E. Chang, An information privacy taxonomy for collaborative environments, Inf. Manag. Comput. Secur. 14 (2006) 382–394, http://dx.doi.org/10.1108/09685220610690835.

[41] C. Kalloniatis, E. Kavakli, S. Gritzalis, Addressing privacy requirements in system design: The PriS method, Requir. Eng. 13 (3) (2008) 241–255, http://dx.doi.org/10.1007/s00766-008-0067-3.

[42] M. Peixoto, C. Silva, H. Maia, J. Araújo, Towards a catalog of privacy related concepts, in: CEUR Workshop Proceedings, vol. 2584, 2020, p. 6.

[43] A. Schreiber, Right To Privacy and Personal Data Protection in Brazilian Law, in: Data Protection in the Internet, Springer International Publishing, Cham, 2020, pp. 45–54, http://dx.doi.org/10.1007/978-3-030-28049-9_2.

[44] M. Finkelstein, C. Finkelstein, Privacidade e lei geral de proteção de dados pessoais privacy and general personal data protection law, Revista de Direito Brasileira 23 (2020) 284–301, URL https://www.indexlaw.org/index.php/rdb/article/view/5343.

[45] F. Brito, J. Machado, Preservação de Privacidade de Dados: Fundamentos, Técnicas e Aplicações, in: Jornadas De Atualização Em Informática, Sociedade Brasileira de Computação - SBC, Porto Alegre, 2017, p. 40, Ch. 3.

[46] I. Webster, V. Ivanova, L.M. Cysneiros, Reusable knowledge for achieving privacy: A Canadian health information technologies perspective, in: J. Araújo, A.D. Toro, J.F. e Cunha (Eds.), Anais Do WER05 - Workshop Em Engenharia de Requisitos, Porto, Portugal, Junho 13-14, 2005, Editora PUC-Rio, Porto, Portugal, 2005, pp. 112–122.

[47] M. Gharib, M. Salnitri, E. Paja, P. Giorgini, H. Mouratidis, M. Pavlidis, J.F. Ruiz, S. Fernandez, A.D. Siria, Privacy requirements: Findings and lessons learned in developing a privacy platform, in: Proceedings - 2016 IEEE 24th International Requirements Engineering Conference, RE 2016, Vol. 13, IEEE Computer Society, 2016, pp. 256–265, http://dx.doi.org/10.1109/RE.2016.13.

[48] N. Zannone, A Requirements Engineering Methodology for Trust, Security, and Privacy (Ph.D. thesis), University of Trento, 2007.

[49] H. Mouratidis, P. Giorgini, Secure tropos: A security-oriented extension of the tropos methodology, Int. J. Softw. Eng. Knowl. Eng. 17 (2) (2007) 285–309, http://dx.doi.org/10.1142/S0218194007003240.

[50] I. Hadar, T. Hasson, O. Ayalon, E. Toch, M. Birnhack, S. Sherman, A. Balissa, Privacy by designers: Software developers' privacy mindset, Empir. Softw. Eng. 23 (1) (2018) 259–289, http://dx.doi.org/10.1007/s10664-017-9517-1.

[51] A.J. Aberkane, G. Poels, S.V. Broucke, Exploring automated GDPR-compliance in requirements engineering: A systematic mapping study, IEEE Access 9 (2021) 66542–66559, http://dx.doi.org/10.1109/ACCESS.2021.3076921.

[52] A.I. Antón, J.B. Earp, A requirements taxonomy for reducing Web site privacy vulnerabilities, Requir. Eng. 9 (3) (2004) 169–185, http://dx.doi.org/10.1007/s00766-003-0183-z.

[53] A.I. Antón, J.B. Earp, A. Reese, Analyzing Website privacy requirements using a privacy goal taxonomy, in: Proceedings of the IEEE International Conference on Requirements Engineering, Vol. 2002-Janua, 2002, pp. 23–31, http://dx.doi.org/10.1109/ICRE.2002.1048502.

[54] N. Rjaibi, L.B.A. Rabai, Developing a novel holistic taxonomy of security requirements, in: Procedia Computer Science, vol. 62, Elsevier B.V., Berkeley, USA, 2015, pp. 213–220, http://dx.doi.org/10.1016/j.procs.2015.08.442.

[55] D.G. Firesmith, Analyzing and specifying reusable security requirements, in: Proceedings of the 11th International IEEE Conference on Requirements Engineering, RHAS 2003, Vol. 3, 2003, pp. 507–514.

[56] B.A. Kitchenham, S. Charters, Guidelines for Performing Systematic Literature Reviews in Software Engineering, Tech. Rep. EBSE 2007-001, Keele University and Durham University Joint Report, 2007, URL https://www.elsevier.com/_data/promis_misc/525444systematicreviewsguide.pdf.

[57] A.I. Anton, Goal-based requirements analysis, in: Proceedings of the IEEE International Conference on Requirements Engineering, IEEE Computer Society, Colorado Springs, CO, USA, 1996, pp. 136–144, http://dx.doi.org/10.1109/icre.1996.491438.

[58] B.G. Glaser, A.L. Strauss, The Discovery of Grounded Theory: Strategies for Qualitative Research, Aldine Publishing Company, Chicago, 1967.

[59] R.C. Nickerson, U. Varshney, J. Muntermann, A method for taxonomy development and its application in information systems, Eur. J. Inf. Syst. 22 (3) (2013) 336–359, http://dx.doi.org/10.1057/ejis.2012.26.

[60] B. Central, C.M. Nacional, Resolução conjunta n. 1, de 4 de maio de 2020, 2020, p. 24.

[61] S. Éllen Renner Ferrão, E.D. Canedo, G.R.S. Silva, F.F. Mendes, Supplementary Material for Towards a Taxonomy of Privacy Requirements Based on the LGPD and ISO/IEC 29100, Zenodo, 2022, http://dx.doi.org/10.5281/zenodo.6590218.

[62] Exame, Maiores bancos - maiores e melhores, 2021, URL https://mm.exame.com/maiores-bancos/. (Last acess on 06 March 2022).

[63] R. Meis, M. Heisel, Understanding the privacy goal intervenability, in: S. Katsikas, C. Lambrinoudakis, S. Furnell (Eds.), Trust, Privacy and Security in Digital Business, Springer International Publishing, Cham, 2016, pp. 79–94.

[64] U.I. Hernandez, M.V. Martin, F.Á. Rodríguez, R.M. González, F.A.G. Toribio, A requirements taxonomy and rating model for secure and usable B2C/C2C e-commerce websites, in: Fifth IEEE International Conference on Digital Information Management, ICDIM, IEEE, Lakehead University, Thunder Bay, Canada, 2010, pp. 367–372, http://dx.doi.org/10.1109/ICDIM.2010.5664661.

[65] R. Meis, M. Heisel, Computer-aided identification and validation of intervenability requirements, Information 8 (1) (2017) 27, http://dx.doi.org/10.3390/info8010030, URL https://www.mdpi.com/2078-2489/8/1/30.

[66] N. Siegfried, T. Rosenthal, A. Benlian, Blockchain and the industrial internet of things: A requirement taxonomy and systematic fit analysis, J. Enterprise Inf. Manag. ahead-of-print (ahead-of-print) (2020) 23, http://dx.doi.org/10.1108/JEIM-06-2018-0140.

[67] S. Lehnert, A taxonomy for software change impact analysis, in: A. Cleve, R. Robbes (Eds.), Proceedings of the 12th International Workshop on Principles of Software Evolution and the 7th Annual ERCIM Workshop on Software Evolution, EVOL/IWPSE 2011, Szeged, Hungary, September 5-6, 2011, ACM, New York, NY, USA, 2011, pp. 41–50, http://dx.doi.org/10.1145/2024445.2024454.

[68] D. Bolchini, P. Paolini, G. Randazzo, Adding hypermedia requirements to goal-driven analysis, in: Proceedings. 11th IEEE International Requirements Engineering Conference, 2003, IEEE Computer Society, Monterey Bay, CA, USA, 2003, pp. 127–137, http://dx.doi.org/10.1109/ICRE.2003.1232744.

[69] N. Alhirabi, O. Rana, C. Perera, Security and privacy requirements for the internet of things, ACM Trans. Internet Things 2 (1) (2021) 1–37, http://dx.doi.org/10.1145/3437537.

[70] Y. Tang, M.L. Brockman, S. Patil, Promoting privacy considerations in real-world projects in capstone courses with ideation cards, ACM Trans. Comput. Educ. 21 (4) (2021) 1–28, http://dx.doi.org/10.1145/3458038.

[71] S. Azad, C. Martens, Little computer people: A survey and taxonomy of simulated models of social interaction, Proc. ACM Hum.-Comput. Interaction 5 (CHIPLAY) (2021) 16, http://dx.doi.org/10.1145/3474672.

[72] K. Lauenroth, E. Kamsties, O. Hehlert, Do words make a difference? An empirical study on the impact of taxonomies on the classification of requirements, in: Proceedings - 2017 IEEE 25th International Requirements Engineering Conference, RE 2017, Institute of Electrical and Electronics Engineers Inc., Lisbon, Portugal, 2017, pp. 273–282, http://dx.doi.org/10.1109/RE.2017.57.

[73] J. Bhatia, T.D. Breaux, F. Schaub, Mining privacy goals from privacy policies using hybridized task recomposition, ACM Trans. Softw. Eng. Methodol. 25 (3) (2016) http://dx.doi.org/10.1145/2907942.

[74] F. Zafar, A. Khan, A. Anjum, C. Maple, M.A. Shah, Location proof systems for smart internet of things: Requirements, taxonomy, and comparative analysis, Electronics 9 (11) (2020) 1–22, http://dx.doi.org/10.3390/electronics9111776.

[75] A.I.A. Ahmed, A. Gani, S.H.A. Hamid, A. Abdelmaboud, H.J. Syed, R.A.A. Habeeb Mohamed, I. Ali, Service management for iot: Requirements, taxonomy, recent advances and open research challenges, IEEE Access 7 (2019) 155472–155488, http://dx.doi.org/10.1109/ACCESS.2019.2948027.

[76] H. Belani, Towards a usability requirements taxonomy for mobile AAC services, in: 2012 1st International Workshop on Usability and Accessibility Focused Requirements Engineering, UsARE 2012 - Proceedings, Vol. 1, 2012, pp. 36–39, http://dx.doi.org/10.1109/UsARE.2012.6226789.

[77] A. Abdelmaboud, The internet of drones: Requirements, taxonomy, recent advances, and challenges of research trends, Sensors 21 (17) (2021) http://dx.doi.org/10.3390/s21175718.

[78] O. Gordieiev, V. Kharchenko, Profile-oriented assessment of software requirements quality: Models, metrics, case study, Int. J. Comput. 19 (4) (2020) 656–665, http://dx.doi.org/10.47839/ijc.19.4.2001, URL https://computingonline.net/computing/article/view/2001.

[79] B. Chen, Q. Dong, A taxonomy system for information system requirements, in: Z. Zhong (Ed.), Proceedings of the International Conference on Information Engineering and Applications, IEA 2012, Springer London, London, 2013, pp. 633–643.

[80] R. MacRuairi, M.T. Keane, G. Coleman, A wireless sensor network application requirements taxonomy, in: 2008 Second International Conference on Sensor Technologies and Applications, Sensorcomm 2008, IEEE Computer Society, Cap Esterel, France, 2008, pp. 209–216, http://dx.doi.org/10.1109/SENSORCOMM.2008.73.

[81] M. Calderón C., A taxonomy of software security requirements, Rev. Avances en Sistemas e Inform. 4 (2007) 44–53.

[82] L. Cheikhi, A. Abran, W. Suryn, Harmonization of usability measurements in ISO9126 software engineering standards, in: 2006 IEEE International Symposium on Industrial Electronics, Vol. 4, IEEE Computer Society, Montreal, QC, Canada, 2006, pp. 3246–3251, http://dx.doi.org/10.1109/ISIE.2006.296137.

[83] C. Jinling, S. Tong, L. Chuncan, S. Tao, Modeling E-commerce website quality with quality function deployment, in: 2009 IEEE International Conference on E-Business Engineering, IEEE Computer Society, Macau, China, 2009, pp. 417–422, http://dx.doi.org/10.1109/ICEBE.2009.65.

[84] M.A. Shaikh, A.H. Al-Badi, A.H. Al-Elaiwi, A. Al-Ameri, J.A. Whittaker, E-commerce need analysis via quality function deployment, in: IEMC'01 Proceedings. Change Management and the New Industrial Revolution. IEMC-2001 (Cat. No.01CH37286), IEEE Computer Society, Albany, NY, USA, 2001, pp. 317–322, http://dx.doi.org/10.1109/iemc.2001.960550.

[85] D.B. Parker, Fighting Computer Crime: A New Framework for Protecting Information, in: Computer Security Handbook, Wiley, New York, USA, 1998, p. 512.

[86] D. Firesmith, Specifying reusable security requirements, J. Object Technol. 3 (1) (2004) 61–75, http://dx.doi.org/10.5381/jot.2004.3.1.c6.

[87] N.R. Mead, T. Stehney, Security quality requirements engineering (SQUARE) methodology, in: Proceedings of the 2005 Workshop on Software Engineering for Secure Systems—Building Trustworthy Applications, SESS '05, Association for Computing Machinery, New York, NY, USA, 2005, pp. 1–7, http://dx.doi.org/10.1145/1083200.1083214.

[88] T. Christian, N. Mead, Security Requirements Reusability and the SQUARE Methodology, Tech. Rep. CMU/SEI-2010-TN-027, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, 2010, URL http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=9389.

[89] J. Jrjens, Secure Systems Development with UML, Springer-Verlag, Berlin, Heidelberg, 2010.

[90] J. Castro, M. Kolp, J. Mylopoulos, Towards requirements-driven information systems engineering: The tropos project, Inf. Syst. 27 (6) (2002) 365–389, http://dx.doi.org/10.1016/S0306-4379(02)00012-1, URL https://www.sciencedirect.com/science/article/pii/S0306437902000121.

[91] A. Kaspary, O Verbo Na Linguagem JuríDica: Acepções E Regimes, Livraria do Advogado Editora, Porto Alegre, BRA, 2021.

[92] C. Wohlin, P. Runeson, M. Hst, M.C. Ohlsson, B. Regnell, A. Wessln, Experimentation in Software Engineering, Springer Publishing Company, Incorporated, Sweden, 2012.