





A Comprehensive Review of Techniques, Methods, Processes, Frameworks, and Tools for Privacy Requirements

Stefano Luppi Spósito  [University of Brasília (UnB), Department of Computer Science, Brasília–DF, Brazil | stefanoluppi@hotmail.com]



João Francisco Gomes Targino  [University of Brasília (UnB), Department of Computer Science, Brasília–DF, Brazil | targino.joao@gmail.com]


Geovana Ramos Sousa Silva  [University of Brasília (UnB), Department of Computer Science, Brasília–DF, Brazil | geovannna.1998@gmail.com]

Laerte Peotta  [University of Brasília (UnB), Brasília–DF, Brazil | peotta@gmail.com]

Daniel de Paula Porto  [University of Brasília (UnB), Department of Computer Science, Brasília–DF, Brazil | daniel.porto@unb.br]

Fábio Lúcio Lopes Mendonça  [University of Brasília (UnB), Brasília–DF, Brazil | fabio.mendonca@unb.br]

Edna Dias Canedo   [University of Brasília (UnB), Department of Computer Science, Brasília–DF, Brazil | ednacanedo@unb.br]

 Universidade de Brasília (UnB), Campus Darcy Ribeiro - Prédio CIC/EST, CEP 70910-900 - Brasília, DF - Brasil

Received: 30 November 2024 • **Accepted:** 12 May 2025 • **Published:** 19 August 2025

Abstract Context: Requirements Engineering (RE) relies on the collaboration of various roles—such as requirements engineers, stakeholders, and developers—and various techniques, methods, processes, frameworks, and tools. This makes RE a highly human-dependent process that benefits greatly from tool support. Understanding how these techniques, methods, processes, frameworks, and tools are applied across RE phases could provide valuable insights into ways to enhance the RE process, contributing to more successful outcomes. **Objective:** The primary objective of this study is to identify the techniques, methods, processes, frameworks, and tools applied across different requirements engineering phases—such as elicitation, analysis, specification, validation, and management—to address privacy requirements. **Method:** We conducted a systematic literature review (SLR) and identified 125 primary studies, and we also conducted a survey with 37 practitioners. **Results:** Our review identified a range of techniques, methods, processes, frameworks, and tools for addressing privacy requirements. Most studies were conducted in academic contexts, with the most frequently used tools being: PriS Method, Secure Tropos, LINDDUN, i* (i-star), STRAP (Structured Analysis for Privacy), Privacy by Design (PbD), and SQUARE. Additionally, over 75% of the studies applied these tools in the privacy requirements elicitation phase. In the industry, most of the techniques identified in the literature are not known or used by practitioners. **Conclusion:** This study provides a comprehensive analysis of techniques and tools for privacy requirements in RE, revealing a strong focus on academic contexts with limited industry application. Future research should explore the scalability and effectiveness of these tools in real-world environments, as well as the reasons why practitioners do not use them.

Keywords: Privacy Requirements, Techniques, Methods, Processes, Frameworks, Tools

1 Introduction

In today's increasingly digital world, privacy has become a central concern in software development Cheung and Liu (2023); Golda *et al.* (2024). As the volume of personal data processed by applications and systems grows, ensuring privacy is a legal requirement and a fundamental ethical responsibility. The challenge of integrating privacy into software development lies in identifying the appropriate techniques, methods, processes, frameworks, and tools that can effectively address privacy concerns throughout the software life-cycle Canedo *et al.* (2023, 2021a).

From elicitation and managing requirements to the final stages of development and deployment, privacy must be considered at every stage to avoid potential risks, breaches, and non-compliance with regulations such as the General

Data Protection Regulation (GDPR) Parliament and Council (2018) and the Brazilian General Data Protection Law (LGPD) Brasil (2018). Additionally, the interest in Artificial Intelligence (AI)-based systems has been growing accelerated, both among software development teams and society at large. As a result, privacy concerns have also increased at the same rate Cheung and Liu (2023); Golda *et al.* (2024).

As AI technologies are increasingly integrated into various applications, from personalized services to predictive analytics, the amount of sensitive data being processed has surged, raising significant privacy and security challenges. This intensifies the need for robust privacy measures and privacy-aware design in AI systems to ensure that user data is handled responsibly and in compliance with evolving regulations Golda *et al.* (2024). One of the critical aspects of addressing privacy concerns in software development is the

application of effective requirement engineering techniques. In particular, understanding and applying existing techniques from the engineering of requirements field, such as elicitation, specification, validation, and management, is essential for ensuring that privacy requirements are adequately defined, prioritized, and incorporated into the system design. These techniques provide structured approaches for identifying privacy needs, assessing potential privacy risks, and ensuring privacy is maintained throughout the development process Canedo *et al.* (2023).

Privacy requirements must be addressed from the early stages of software development. This includes identifying, analyzing, specifying, validating, and managing these requirements to prevent data breaches and ensure compliance with regulations such as the GDPR Parliament and Council (2018) and Brazil's LGPD Sâmmara ellen Renner Ferrão (2024); Canedo *et al.* (2021b). Techniques from Requirements Engineering (RE) offer structured approaches to this process and can help identify privacy needs, assess risks, and guide design decisions. However, defining and managing privacy requirements remains a complex task, often hindered by the difficulty of translating legal obligations into technical specifications and balancing them with other system goals. Given this complexity, it is essential to investigate how privacy-related techniques, methods, processes, frameworks, and tools are applied across the RE phases.

We conducted a Systematic Literature Review (SLR) to identify and analyze 125 primary studies that propose or apply approaches for addressing privacy requirements across RE phases. Complementing the SLR, we also carried out a survey with 37 industry practitioners to understand the practical adoption of these approaches and the challenges faced in real-world scenarios. These two methods allowed us to compare academic and industrial perspectives and to assess the alignment — or lack thereof — between them.

The main goal of this study is to identify and classify the techniques, methods, processes, frameworks, and tools used across the different RE phases to support the definition and implementation of privacy requirements. Additionally, we aim to assess how these approaches are applied in both academic and industrial contexts, identify the main challenges encountered in practice, and evaluate the applicability and scalability of existing solutions. By synthesizing evidence from the literature and industry, this study contributes to bridging the gap between theory and practice and supports the development of privacy-aware software systems that comply with current data protection regulations.

Our findings reveal that SQUARE, Secure Tropos, PriS, i* (i-Star), LINDDUN, STRAP, and Privacy by Design are the most commonly used techniques. Most of these techniques are applied exclusively during the requirements elicitation phase. The article is structured as follows: In Section 2 discusses related work relevant to this research, along with background information and key concepts necessary for understanding the study. Section 3 presents the research methodology, detailing the systematic literature review (SLR) process, from formulating the research questions to the final selection of studies. Section 4 presents the results of the SLR, highlighting the main characteristics of the collected studies and providing answers to the identified research questions. Sec-

tion 5 describes the findings from the survey conducted in this study, while Section 6 offers a general discussion of the results obtained throughout the SLR. Additionally, Section 7 outlines the threats to the validity of this study, identified during the systematic review process and result analysis. Finally, Section 8 presents the overall conclusions of the study.

2 Background and Related Work

2.1 Foundational Knowledge

Privacy is regarded as a multifaceted and dynamic concept that extends beyond the mere control of individuals over their personal information Gharib *et al.* (2017). It encompasses the fundamental right of every individual to manage their data and make decisions about how, when, and with whom this information is shared Kalloniatis *et al.* (2005). Contemporary privacy is not limited to protection against state or corporate surveillance; it also includes the broader principle of informational self-determination Silva *et al.* (2018).

Veseli *et al.* (2019) proposed three domains in which privacy engineers are responsible for exercising and promoting privacy: 1) User Sphere — this domain encompasses the devices used by the user, emphasizing that each individual should have complete control over their devices and, consequently, over the information contained within them; 2) Recipient Sphere — this refers to the organizational context, where privacy engineers are tasked with minimizing the risks of confidential data leaks and privacy breaches; and 3) Joint Sphere — this consists of companies that hold individuals' personal data. Like the recipient sphere, privacy engineers must minimize the risks of data leaks and employ appropriate tools to ensure data privacy and security.

As early as 2005, Kalloniatis *et al.* (2005) warned about the growing risks to individual privacy worldwide due to the increasing Internet use. The authors emphasized the need for a methodology to address privacy requirements. One of their recommendations was to pursue international harmonization of privacy legislation. However, they also noted a significant challenge: cultural differences would make such harmonization extremely difficult. This prediction has proven accurate, as modern privacy laws across countries share some similarities but remain distinct, making a unified global regulation unfeasible.

Brazilian Data Protection Law (LGPD) Brasil (2018), established by Law No. 13,709/2018, regulates the processing of personal data, both physical and digital, by public and private organizations. The law, inspired by the General Data Protection Regulation (GDPR) Parliament and Council (2018), aims to protect fundamental rights of freedom and privacy, ensuring transparency in using personal information. The LGPD Brasil (2018) and GDPR Parliament and Council (2018) share several principles, emphasizing transparency, necessity, security, and the specific purpose of data use. Additionally, these regulations grant individuals similar rights, such as access, correction, deletion, and portability of their data, along with the right to be informed about using and sharing their information. In addition to the privacy principles outlined and defined in the LGPD Brasil (2018), Alves

and Neves (2021) proposed privacy standards in compliance with the law based on perceptions gathered from interviews with practitioners in the information technology field. This was motivated by the need to create standards to identify principles and ensure compliance with the respective privacy regulations.

Privacy requirements refer to the conditions, standards, and regulations that protect personal data and safeguard individuals' privacy rights. These requirements often arise from legal frameworks such as the GDPR and the LGPD. They aim to define how personal data should be collected, processed, stored, and shared, ensuring transparency, accountability, and the right to privacy for individuals Canedo *et al.* (2023). The primary goal of privacy requirements engineering is to clearly define and understand a system's privacy requirements, ensuring seamless integration into the system's design and development. This process often involves conducting risk analyses, threat assessments, and privacy impact assessments to identify and address potential privacy risks. Once privacy requirements are identified and defined, the focus shifts to designing solutions that fulfill these requirements, a process known as privacy design engineering. This phase may involve implementing specific technologies or strategies, such as encryption or anonymization, to safeguard user privacy and data. Adopting a risk-based approach further ensures that privacy designs align with established risk management principles Herwanto *et al.* (2024a). There are several techniques for designing privacy requirements. Notario *et al.* (2015) approached this from two perspectives: a goal-oriented approach and a risk-based approach. The goal-oriented perspective focuses on deriving privacy principles and establishing them as system requirements. Privacy or data protection goals are often derived from fundamental privacy principles and legal frameworks. Hansen *et al.* (2015) identified six core data protection goals: Confidentiality, Integrity, Availability, Unlinkability, Transparency, and Inter-venability.

2.2 Related Work

Sâmmara ellen Renner Ferrão (2024) proposed a taxonomy of privacy requirements to support software development teams in overcoming legal compliance challenges, particularly those related to LGPD and ISO/IEC 29100. Using a systematic literature review (SLR), the authors identified 10 primary studies as the foundation for their work. Applying the Goal-Based Requirements Analysis Method (GBRAM) and Grounded Theory, they formulated 129 privacy requirements, categorized into 10 groups aligned with LGPD principles and distributed across 5 application contexts: Software, Research, Governance, Public Management, and Infrastructure. The taxonomy was validated through a case study involving Open Banking projects at three major Brazilian banks, demonstrating its utility in guiding software teams in effectively specifying privacy requirements.

Frej *et al.* (2024) developed an automated tool to streamline the assessment and implementation of LGPD principles, aiming to assist organizations in ensuring compliance with the privacy requirements mandated by the law. Testing of the tool demonstrated its efficiency and accessibility, offer-

ing a practical solution to address the regulatory challenges posed by the LGPD.

Camêlo and Alves (2023) proposed a catalog of privacy patterns and a guide named G-Priv to support the specification of privacy requirements in compliance with the LGPD. They conducted a survey with 18 professionals to evaluate G-Priv, which was easy to understand, particularly in defining the roles and responsibilities of stakeholders involved in the guide's four stages. Survey participants also highlighted the guide's usability and efficiency, considering it a valuable tool to assist requirements analysts in specifying privacy requirements aligned with LGPD compliance.

Various methodologies contribute to a body of knowledge encompassing methods, tools, privacy knowledge bases, models, documentation, and other elements designed to help software engineers create privacy-preserving systems. Caiza *et al.* (2019) emphasized an urgent need for further research to identify methods that support the development of systems focused on data privacy. The authors highlighted the significance of automated tools for broader industrial adoption. This research addresses this gap by investigating the techniques, methods, processes, frameworks, and tools used in Requirements Engineering for elicitation, analysis, specification, validation, and management of privacy requirements.

3 Research Methodology

We conducted a Systematic Literature Review (SLR) to identify and synthesize existing primary research studies on the techniques, methods, processes, frameworks, and tools in Requirements Engineering (RE) used in both literature and industry for the elicitation, analysis, specification, validation, and management of privacy requirements. This SLR aims to comprehensively analyze current research addressing specific questions in the field. We followed the structured methodology outlined in Kitchenham and Charters' guidelines Keele *et al.* (2007), ensuring an unbiased, repeatable approach to assess all available evidence from published primary studies. Our findings offer valuable insights for RE researchers and practitioners by examining study methodologies, proposed solutions, and their application in both industry and academia and identifying research gaps to suggest critical areas for further exploration in privacy requirements within the RE field.

The first and second authors developed the detailed review protocol, conducted extensive searches, filtered studies, and performed data extraction and analysis, all under the close supervision of the third and fourth authors, who are highly experienced in conducting SLRs in software engineering. To synthesize the extracted data from the final set of 125 studies, we applied a meta-analysis technique Shelby and Vaske (2008). This approach, commonly used in SLRs, involves analyzing a large collection of structured data from individual studies to integrate and summarize their key findings.

3.1 Research Questions

The set of research questions (RQs) was developed using Wohlin's approach Wohlin *et al.* (2012), focusing on the

intervention, population, outcomes of interest, and context in which the intervention is applied. This approach is explained as PICOC (Population, Intervention, Comparison, Outcomes, and Context) in the guidelines by Kitchenham and Charters Keele *et al.* (2007). Using the PICOC framework, the following RQs were formulated, as shown in Table 1.

- RQ.1 What techniques, methods, processes, frameworks, and tools have been used in the literature to elicit, analyze, specification, validate, and manage privacy requirements in different contexts?
- RQ.2 How are the techniques, methods, processes, frameworks, and tools identified in the literature and industry used in the phases of requirements engineering for privacy?
- RQ.3 What are the challenges in eliciting privacy requirements?

The responses to the research questions will help identify the techniques, methods, processes, frameworks, and tools, along with the challenges noted in the literature on privacy requirements and in the industry and their applications at each stage of Requirements Engineering.

3.2 Search Strategy

First, we developed a search string by selecting key search terms from the PICOC framework (see Table 1). Using these identified terms, we created multiple search strings executed across four online databases (see Table 2). We primarily employed Boolean operators in constructing the final search string, specifically AND and OR. The AND operator combined key terms, and the OR operator connected synonyms. We conducted several iterations of searches to optimize the search strings for each database. During this process, we utilized various search techniques, such as wildcards and stemming, as recommended in the help sections of the digital libraries. The most effective search strings for each online database were selected based on their ability to yield the most relevant primary studies. We did not impose any specific time range for the search, as our objective was to assess the distribution of all identified primary studies.

Population	Techniques, methods, processes, frameworks, and tools in requirements engineering for identification, specification, validation, verification, and management.
Intervention	The techniques, methods, processes, frameworks, and tools utilized to achieve the desired outcome.
Comparison	This does not apply, as the objective of this research is not to compare methods.
Outcomes	Techniques, methods, processes, frameworks, and tools used in requirements engineering for identifying, specifying, validating, verifying, and managing privacy requirements.
Context	Requirements Identification/ Requirements Specification/ Requirements Validation/ Requirements Verification/ Requirements Management/ Requirements Engineering.

Table 1. PICOC for Research Questions

We employed two search procedures to identify relevant research papers for the SLR: automatic and manual. The automatic search was conducted using the search engines of scientific databases, while the manual search involved scanning the reference lists of primary studies obtained from the

automatic search. We selected the scientific databases listed in Table 2 for their comprehensive coverage of papers in computer science and requirements engineering (RE) studies. To address the limitations of each database, we refined our search string to align with the specific requirements and configurations of each database's search engine (see Table 2). To ensure relevance, each search string was adjusted and executed multiple times. We then randomly selected 8-10 papers from each database to verify that the resulting studies were the most relevant for our review. The finalized search strings are provided in Table 2. Additionally, we performed manual searches using backward and forward snowballing techniques with the retrieved primary studies, which enabled us to discover further relevant studies for our SLR, as recommended by Achimugu *et al.* (2014).

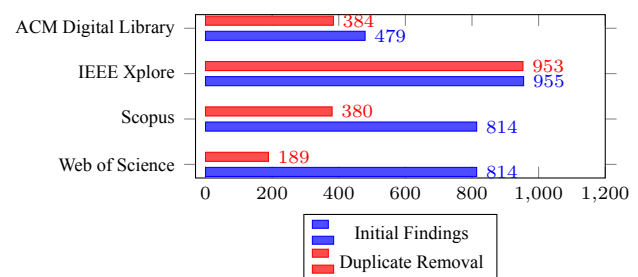


Figure 1. Number of Studies Identified and Selected by Digital Database

After the initial data extraction step, all BibTeX files were downloaded and stored locally. Duplicate entries were then managed using the slr-manager tool, which generated a new file containing only unique BibTeX entries. After removing duplicates, 1,906 studies remained, as shown in Figure 1.

The studies were selected based on well-defined inclusion (IC) and exclusion criteria (EC) established during the protocol preparation for this SLR. We applied two inclusion and four exclusion criteria to filter the identified papers, ensuring the final selection aligned with our review objectives and research questions. These criteria were refined throughout the search and filtering processes to create an unbiased set of papers. The finalized criteria were applied to all downloaded full-text papers to select the most relevant studies. Consistent with standard practices in systematic literature reviews (SLRs), we excluded review papers, workshop or magazine articles, and grey literature from our analysis.

- (IC1) The study presents techniques, methods, processes, frameworks, or tools related to software privacy requirements;
- (IC2) The study is a peer-reviewed research article (i.e., a journal article or conference paper).
- (EC1) The study is outside the context of requirements engineering (e.g., software architecture, distributed systems, VANETS).
- (EC2) The study is not a full paper (e.g., fewer than 6 pages).
- (EC3) The study is not a primary work (e.g., a literature review or a duplicated/extended paper).
- (EC4) The study is not written in a language understood by the authors (e.g., a language other than English, Portuguese, or Spanish).

According to the inclusion and exclusion criteria established, we classified all studies as follows: 1) Rejected -

Database	Search String
Original String	`privacy requirements" AND (elicitation OR identification OR gathering OR specification OR analysis OR validation OR verification OR documentation OR management OR engineering) AND (method OR methodology OR technique OR process OR tool OR framework)
ACM Digital Library	[All:`privacy requirements"] AND [[All: elicitation] OR [All: identification] OR [All: gathering] OR [All: specification] OR [All: analysis] OR [All: validation] OR [All: verification] OR [All: documentation] OR [All: management] OR [All: engineering]] AND [[All: method] OR [All: methodology] OR [All: technique] OR [All: process] OR [All: tool] OR [All: framework]]
IEEE Xplore	`privacy requirements" AND (elicitation OR identification OR gathering OR specification OR analysis OR validation OR verification OR documentation OR management OR engineering) AND (method OR methodology OR technique OR process OR tool OR framework)
Scopus	TITLE-ABS-KEY (`privacy requirements" AND (elicitation OR identification OR gathering OR specification OR analysis OR validation OR verification OR documentation OR management OR engineering) AND (method OR methodology OR technique OR process OR tool OR framework))
Web of Science	`privacy requirements" AND (elicitation OR identification OR gathering OR specification OR analysis OR validation OR verification OR documentation OR management OR engineering) AND (method OR methodology OR technique OR process OR tool OR framework)

Table 2. Research String per Database

ABS: The study was rejected based on its abstract, as it was found to meet one of the rejection criteria or was not related to privacy or privacy requirements elicitation; 2) Rejected - FText: The study was rejected for failing to meet the minimum page count required for a full paper, not being a primary work, or lacking content that aligns with the acceptance criteria; 3) Rejected - QA: The study does not meet the quality criteria defined in this research, as outlined in Section 3.3; and Accepted: The study meets all requirements.

3.3 Quality Assessment

We defined six criteria for the identified studies' Quality Assessment (QA). These criteria were essential to ensure that the selected studies significantly contribute to the understanding and advancement of privacy requirements practices. We developed a scoring mechanism with predefined questions related to paper quality that includes five levels of evaluation, ranging from low to high: very poor (1), inadequate (2), moderate (3), good (4), and excellent (5). Each paper was assigned a score from 1 to 5 based on responses to the following questions:

- (QA1) **Clarity in Application Context Definition:** Does the study clearly describe the context in which the privacy requirements techniques or tools were applied, such as the requirements engineering phase or the type of system or application?
- (QA2) **Methodological Rigor in the Description of Techniques and Methods:** Does the study provide a detailed and methodologically rigorous description of the privacy requirements techniques, methods, processes, frameworks, or tools used?
- (QA3) **Empirical or Theoretical Evidence:** Does the study present empirical evidence (such as case studies, experiments, or evaluations) or a solid theoretical basis supporting the use of the proposed techniques or tools for privacy requirements?
- (QA4) **Effectiveness Evaluation:** Does the study discuss or evaluate the effectiveness of the techniques, methods, or tools in practice? Are data or examples provided demonstrating how the techniques were successful or what challenges were encountered?
- (QA5) **Consideration of Specific Privacy Aspects:** Does the study address specific aspects of privacy requirements, such as compliance with regulations (e.g., GDPR,

LGPD), protection of sensitive data, or access control, in a detailed and relevant manner?

(QA6) Relevance and Practical Applicability: Does the study discuss the practical relevance of the techniques or tools in various application contexts and whether they can be generalized or adapted to other environments or industries?

(QA7) Transparency and Replicability: Does the study present the results transparently, providing sufficient detail for other researchers or practitioners to replicate the techniques or methods in similar contexts?

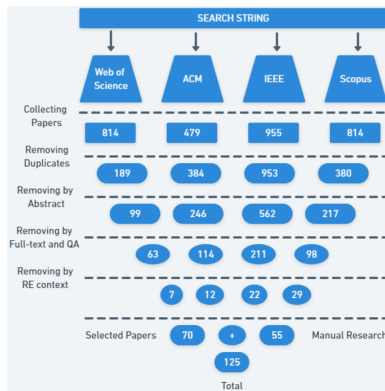
This scoring mechanism was applied to the final set of papers, allowing us to assess the quality of the filtered studies. We identified six low-quality studies with an average score of less than 3 and excluded them from the paper set, resulting in a final count of 125 papers. It is important to emphasize that all criteria were equally important during the evaluation of the studies; however, special attention is given to criteria QA4 and QA7. This is because the techniques, methods, processes, and frameworks must demonstrate proven effectiveness and the possibility of replication. Additionally, a clear explanation is required for any unresolved challenges related to the selected study.

3.4 Conducting the SLR

During the SLR process, 1,904 studies were analyzed. Out of these, 782 studies were eliminated based on their abstracts and titles, 426 were excluded due to their content, and 93 were removed according to text quality criteria, where the techniques presented in the respective texts were not comprehensible. Ultimately, 486 studies were selected for a more detailed evaluation, in which techniques, methods, processes, frameworks, or tools related to requirements engineering were identified and cataloged. In the end, 70 studies were classified as "Accepted," meeting the acceptance criteria and addressing the research questions. Additionally, 55 studies were found manually through searches conducted in the DBLP database using the string "Privacy Requirements," as well as searches in the published studies of the (WER), (Requirements Engineering Conference) e (REFSQ), bringing the total to 125 studies classified as accepted after this review.

Figure 2 visually illustrates the stages of the study selection process. "Collecting Papers" represents the initial stage

of gathering studies retrieved from digital databases, along with the number of studies at each phase of the process. “Removing Duplicates” denotes eliminating duplicate studies and the resulting counts. “Removing by Abstract” indicates the number of papers remaining after applying selection criteria to the titles and abstracts. “Removing by Full-text and QA” refers to the number of studies left after applying the selection criteria to the full text of the studies. “Removing by RE Context” involves the removal of papers that addressed privacy but had no connection to the requirements engineering process. Finally, “Selected Papers” presents the studies chosen for data extraction, while “Manual Research” indicates the number of studies selected through manual searches.



QA = quality assessment RE = Requirements Engineering

Figure 2. Stages of the Study Selection Process

During the data extraction procedure, the researchers carefully reviewed the primary studies. A peer-review process was implemented, where two researchers extracted data from the same studies, and a third researcher resolved disagreements. To align the researchers’ understanding in addressing the research questions, we extracted pilot data using a small sample of papers. The pilot involved five randomly selected primary studies, and the researchers discussed any discrepancies found in their individual results. All relevant information from each study was compiled in a table, as presented in Table 1. Selected Papers (2005-2024) (available in the Supplementary Material on Zenodo).

All selected primary studies were published between 2005 and 2024. Figure 3 illustrates the distribution of these studies by publication year. From 2005 to 2017, the annual number of publications remained low. However, starting in 2018, there has been a gradual increase in the number of studies. This trend suggests a growing interest and productivity in privacy research, likely driven by the implementation of significant data privacy laws, such as the General Data Protection Regulation (GDPR) Parliament and Council (2018) and Brazil’s General Data Protection Law (LGPD) Brasil (2018). Please note that the paper list was compiled in early 2024, so additional studies may have been published since our search.

To ensure consistent analysis and data extraction from each study, we created a Google Form containing 36 questions (Table 3). The questions were formulated based on our research questions (RQs) and adapted from the framework proposed by Hidellaarachchi *et al.* (2021). Table 1. Selected Papers (2005-2024) available in the supplementary material

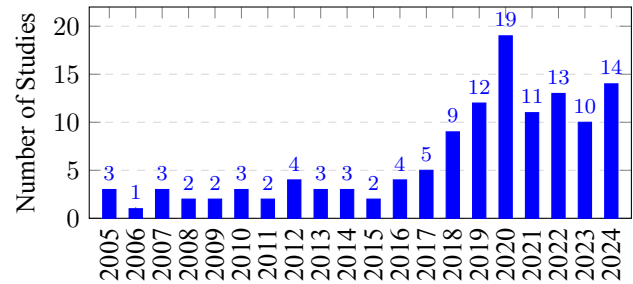


Figure 3. Number of selected primary studies by year

on Zenodo lists the primary studies identified as relevant for answering each RQ. In the following sections, we will discuss the answers to our RQs in detail.

4 SLR Results

Based on the previously presented selection criteria, data from the 125 accepted studies were extracted clearly and objectively using the extraction form. These results allowed us to establish the relationship between all studies and their respective research questions and identify the primary techniques, methods, processes, frameworks, and tools used in the privacy requirements elicitation process and, consequently, in the requirements engineering process. It is important to note that some studies did not provide sufficiently clear data to fill out all fields of the extraction form. However, this was not considered a limitation, as the acceptance and quality criteria had already been applied to these studies, and they were classified as accepted.

Figure 4 illustrates the number of studies categorized by the methods used in the selected research. Case studies represented the largest category, with 29 primary studies employing this method to address privacy requirements. The second most common method was documentation analysis, utilized in 22 studies. Frameworks and modeling were each observed in 20 studies. Additionally, 15 studies employed surveys, while 10 used other unspecified methods. Finally, 8 studies utilized interviews as their primary method.

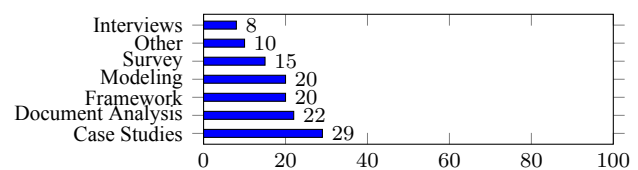


Figure 4. Number of Studies by Methods

Of the 125 primary studies, 40 focused on one of the requirements engineering phases, presenting specific tools for their respective phases or indicating how their results would impact them. These studies are: Sangaroonsilp *et al.* (2023b), Kalloniatis *et al.* (2008), Kalloniatis *et al.* (2012), Islam *et al.* (2015), Miyazaki *et al.* (2008), Kalloniatis *et al.* (2005), Silva *et al.* (2018), Spiekermann and Cranor (2008), Peixoto *et al.* (2023), Herwanto *et al.* (2024d), Salnitri *et al.* (2020), Peixoto *et al.* (2019), Hörbe and Hötendorfer (2015), Stary and Heininger (2022), Kavakli *et al.* (2007), Stach and Steimle (2019), Aslam *et al.* (2021), Zhao *et al.* (2024), Diamantopoulou *et al.* (2017), Peixoto *et al.* (2020), Savola (2010), Ferrão *et al.* (2024), Alkubaisy *et al.* (2019),

ID	Extraction Criteria
1	Study ID
2	Source Type
3	Paper Title
4	Published Year
5	The number of citations of the study?
6	What is the aim/motivation/goal of the study?
7	What research question does the study answer?
8	Subjects used in the study: Professionals or Undergraduates (Requirement Engineers/ Stakeholders/ Clients/ Students)?
9	What are the TECHNIQUES that are considered in the study?
10	What are the METHODS that are considered in the study?
11	What are the PROCESSES that are considered in the study?
12	What are the FRAMEWORKS that are considered in the study?
13	What are the TOOLS that are considered in the study?
14	What are the other things (not techniques, methods, processes, frameworks and tools) that are considered in the study?
15	What phases of the RE are considered in the study (Elicitation/ Specification/ Analysis/ Validation/ Management)?
16	Does the research identify the most affected RE phase by privacy requirements? (Yes/ No)
17	If Yes, What is the most affected RE Phase(s)?
18	Does the study use any existing domain models related to privacy requirements? (Yes/ No)
19	If yes, what are the existing domain models used in studies to identify privacy requirements?
20	Method used in the study(s)? (Case studies/Interviews/ Modelling /framework/ Document analysis/ surveys/ other)
21	Is the study conducted based on academia or industry?
22	The number of participants used in the study
23	What type of data analysis used in the study? (Qualitative/ Quantitative/ Mixed)
24	What are the key research gaps/ future work identified by each study?
25	Does the research focus on identifying the relationship between different privacy requirements? (Yes/ No)
26	If Yes, what are the identified relationships between different privacy requirements?
27	Does the research include how the privacy requirements impact on RE? (Yes/ No)
28	If Yes, what is the nature of the impact of the privacy requirements on RE? (Positive/ Negative/ Both)
29	If Positive, does the study mention the benefits of considering the privacy requirements?
30	If Negative, how it will impact on RE?
31	Does the study suggest any approach to mitigate the negative impact?
32	Main outcome/Results of the study?
33	Does the study come up with a framework/ model as the final outcome?
34	If Yes, what type of framework it is? (Elaborate the developed framework)
35	How do they evaluate their results/ framework/ model?
36	What are the major recommendations of the study?

Table 3. Data Extraction Form.

Ferraris and Gago (2020), Alves and Neves (2021), Ferrao and Canedo (2022), Gramajo *et al.* (2020), Herwanto *et al.* (2024a), Silva and Sarkis (2023), de Sá Sousa *et al.* (2023), Peixoto *et al.* (2024), Alkubaisy *et al.* (2021b), Herwanto *et al.* (2022), Piras *et al.* (2020), Canedo *et al.* (2020), Diamantopoulou *et al.* (2020), Ebrahimi *et al.* (2021), Omitola *et al.* (2022), Amaral *et al.* (2023), Makri *et al.* (2020).

Eighty-eight (88) primary studies were conducted in an academic context, meaning the authors identified or proposed techniques, methods, processes, frameworks, or tools and tested their proposals with students or in hypothetical projects. In contrast, 33 studies were conducted within an industrial context, where authors tested their proposals using real software industry projects. Additionally, 4 studies provided only a literature review of the techniques used and illustrated their application.

Thirty-four (34) studies identified relationships between different privacy requirements. For example, Tsohou *et al.* (2020) assert that privacy requirements should align with security, legal, and acceptance needs, addressing aspects such as privacy by design, consent management, and privacy impact assessments while ensuring compliance with GDPR obligations. Additionally, Herwanto *et al.* (2022) identified privacy as one of six core security requirements within IoT systems, noting that privacy requirements are linked to contexts such as authentication, confidentiality, and access control. Furthermore, fifteen (15) studies highlighted the positive impacts of privacy requirements on requirements engineering, six mentioned negative impacts, and fifty-six (56) studies reported both positive and negative impacts, respec-

tively.

Overall, the primary studies highlighted that the positive impacts of privacy requirements on requirements engineering include enhancing the understanding and fulfillment of stakeholder needs, supporting organizational decision-making Islam *et al.* (2015), guiding software development, and managing regulatory compliance. By integrating privacy from the initial stages, rights violations are prevented, user trust and data transparency are increased, and legal compliance—such as with GDPR and LGPD—is ensured Freund *et al.* (2023), resulting in more secure systems designed with a focus on protecting user data privacy.

Regarding the negative aspects, studies highlight challenges associated with the complexity and confusion of implementing privacy laws like the GDPR, including ambiguous terminology and difficulties in translating legal principles into privacy requirements Huth and Matthes (2019). Another critical issue is the conflict between privacy requirements and other demands, such as identity management, particularly in IoT environments Ferraris and Gago (2020). Additionally, the immutability of technologies like blockchain can complicate compliance with data privacy laws requiring personal data deletion. Studies also indicate that inadequate management of privacy requirements can lead to low-quality software and increase the risk of legal sanctions Piras *et al.* (2020).

4.1 RQ.1. What techniques, methods, processes, frameworks, and tools have been used in the literature to elicit, analyze, specification, validate, and manage privacy requirements in different contexts?

The studies selected in this SLR presented various techniques, methods, processes, frameworks, and tools either proposed or applied within the literature in different stages of Requirements Engineering. However, most studies utilized one or more techniques, methods, processes, frameworks, and tools already established in the literature. Table 4 shows the studies and the respective methods employed in each.

SQUARE The Security Quality Requirements Engineering (SQUARE), developed by the software engineering institute's networked systems survivability (NSS) program, is designed to identify and prioritize security requirements in software projects. Steps in the SQUARE process are Bijwe and Mead (2010): 1. Agree on definitions; 2) Identify Assets and Privacy Goals; 3) Collect Artifacts; 4) Risk Assessment; 5) Select Elicitation Technique; 6) Elicit Security Requirements; 7) Categorize Requirements; 8) Prioritize requirements; and 9) Inspect Requirements. Although the process was originally developed for security requirements, some studies have adapted and used the SQUARE to incorporate and address privacy requirements, such as Miyazaki *et al.* (2008) and Mead *et al.* (2011). Bijwe and Mead (2010) also adapted the SQUARE process for privacy requirements, illustrating how SQUARE, primarily used for security requirements, can be tailored to address privacy concerns. The authors outlined the specific modifications needed at each step of the SQUARE process to effectively align it with privacy requirements.

Secure Tropos The Secure Tropos method Mouratidis and Giorgini (2007) is an extension of the original Tropos methodology Castro *et al.* (2001), designed to integrate security concerns into the development of agent-oriented systems. Initially developed for modeling requirements in multi-agent systems, the method has been expanded to address security requirements from the early stages of requirements engineering to its completion. The Secure Tropos method primarily focuses on security requirements; however, it can also be adapted to encompass privacy requirements. Studies by Mouratidis and Giorgini (2007) and Diamantopoulou *et al.* (2018) evaluated Secure Tropos for eliciting security and privacy requirements in a single scenario. The authors also suggested modifications to enhance the method's applicability across different contexts. Islam *et al.* (2010) applied the Secure Tropos method to elicit privacy and security requirements from laws and regulations related to data privacy.

PriS Method The PriS method is a security requirements engineering approach that integrates privacy requirements from the outset of the software development process Kalloniatis *et al.* (2008). It treats privacy requirements as organizational goals and proposes using privacy process patterns to

describe the impact of privacy requirements on system and business processes. The PriS method identifies the system architecture that best supports these privacy processes. The PriS method follows four main activities: 1) Privacy goal elicitation; 2) Impact analysis; 3) Modeling of affected processes; and 4) Identification of implementation techniques.

i* (i-star) The i* (i-star) framework is a goal- and actor-oriented approach Yu *et al.* (2007). Its primary function is to capture and analyze the strategic interactions between agents or entities responsible for actions within a system, along with the motivations driving these interactions. The framework can be applied across various stages of software development, such as requirements elicitation and analysis, system design, and organizational analysis. Some studies, including Peixoto and Silva (2018), utilize this framework to support and compare their developed frameworks and models. In the evaluation process of the framework developed in this study, i* was one of three frameworks used for comparison.

LINDDUN The LINDDUN methodology is a systematic framework designed to analyze and address system privacy issues, focusing primarily on incorporating privacy from the early stages of system development. This approach facilitates identifying potential privacy threats Deng *et al.* (2011). LINDDUN is based on decomposing privacy threats into seven main categories, represented by the acronym from which it derives its name: 1) Linkability: Focuses on the ability to link two or more activities or attributes to a single individual; 2) Identifiability: Refers to the ability to identify an individual within a dataset; 3) Non-repudiation: Ensures that an individual cannot deny having performed a particular action; 4) Detectability: Involves an attacker's ability to detect whether specific data is present in a dataset; 5) Disclosure of Information: Relates to the leakage of personal information, even when it is not directly associated with an individual; 6) Unawareness: Addresses an individual's lack of awareness regarding how their data is being used; and 7) Non-compliance: Concerns the failure to adhere to privacy laws and regulations. It is also important to note that this methodology provides a detailed taxonomy of privacy threats and their impacts and suggested mitigation techniques tailored to the system development scenario and identified risks. Some studies use the LINDDUN methodology as both a foundation and a reference, as demonstrated in the study by Veseli *et al.* (2019). This study identifies 56 privacy threats categorized within the LINDDUN framework and provides recommendations for appropriate mitigation mechanisms for each identified threat.

STRAP (Structured Analysis for Privacy) The STRAP framework Jensen *et al.* (2005) is a lightweight, structured approach for analyzing privacy vulnerabilities in system design. This framework uses goal-oriented analysis to identify privacy vulnerabilities, categorize them, and propose solutions or strategies to mitigate them. The STRAP framework consists of four steps: 1) Analysis: System actors, goals, and components are identified, and a set of analytical questions is applied to each goal and sub-goal; 2) Refinement: Once

Name	Type	References
Security quality requirements engineering (SQUARE)	Process	Bijwe and Mead (2010), Miyazaki <i>et al.</i> (2008), Peixoto <i>et al.</i> (2023), Mead <i>et al.</i> (2011), Mai <i>et al.</i> (2018), Salnitri <i>et al.</i> (2020), Pattakou <i>et al.</i> (2017), Pattakou <i>et al.</i> (2018)
Secure Tropos	Method	Mouratidis <i>et al.</i> (2020), Argyropoulos <i>et al.</i> (2017), Mouratidis <i>et al.</i> (2012), Huth and Matthes (2019), Alkubaisy <i>et al.</i> (2021a), Ganji <i>et al.</i> (2015), Peixoto <i>et al.</i> (2023), Kalloniatis <i>et al.</i> (2013), Diamantopoulou <i>et al.</i> (2018), Kavakli <i>et al.</i> (2007), Mouratidis and Giorgini (2007), Pattakou <i>et al.</i> (2017), Peixoto and Silva (2018), Peixoto <i>et al.</i> (2020), Islam <i>et al.</i> (2010), Gharib <i>et al.</i> (2017), Pattakou <i>et al.</i> (2018), Ferraris and Gago (2020), Diamantopoulou <i>et al.</i> (2020)
PriS	Method	Mouratidis <i>et al.</i> (2020), Argyropoulos <i>et al.</i> (2017), Kalloniatis <i>et al.</i> (2008), Mouratidis <i>et al.</i> (2012), Kalloniatis <i>et al.</i> (2012), Huth and Matthes (2019), Beckers (2012), Ganji <i>et al.</i> (2015), Kalloniatis <i>et al.</i> (2005), Peixoto <i>et al.</i> (2023), Kalloniatis <i>et al.</i> (2013), Kavakli <i>et al.</i> (2006), Mead <i>et al.</i> (2011), Salnitri <i>et al.</i> (2020), Dias Canedo <i>et al.</i> (2020), Kalloniatis <i>et al.</i> (2009), Gjermundrød <i>et al.</i> (2016), Kavakli <i>et al.</i> (2007), Pattakou <i>et al.</i> (2017), Diamantopoulou <i>et al.</i> (2017), Coles <i>et al.</i> (2018), Pattakou <i>et al.</i> (2018), Kalloniatis <i>et al.</i> (2007)
i* (i-star)	Framework	Deng <i>et al.</i> (2011), Mouratidis <i>et al.</i> (2020), Mouratidis <i>et al.</i> (2012), Huth and Matthes (2019), Ganji <i>et al.</i> (2015), Salnitri <i>et al.</i> (2020), Kavakli <i>et al.</i> (2007), Peixoto and Silva (2018), Peixoto <i>et al.</i> (2020), Pattakou <i>et al.</i> (2018)
LINDDUN	Method	Deng <i>et al.</i> (2011), Manna <i>et al.</i> (2022), Huth and Matthes (2019), Beckers (2012), Veseli <i>et al.</i> (2019), Peixoto <i>et al.</i> (2023), Pattakou <i>et al.</i> (2017), Coles <i>et al.</i> (2018), Pattakou <i>et al.</i> (2018), Omitola <i>et al.</i> (2022), Herwanto <i>et al.</i> (2024b)
STRuctured Analysis for Privacy (STRAP)	Framework	Kalloniatis <i>et al.</i> (2008), Mouratidis <i>et al.</i> (2012), Huth and Matthes (2019), Ganji <i>et al.</i> (2015), Gharib <i>et al.</i> (2021), Kavakli <i>et al.</i> (2007), Jensen <i>et al.</i> (2005), Pattakou <i>et al.</i> (2018)
Privacy By Design (PbD)	Method	Manna <i>et al.</i> (2022), Ganji <i>et al.</i> (2015), Freund <i>et al.</i> (2023), Kalloniatis <i>et al.</i> (2005), Perera <i>et al.</i> (2020), Veseli <i>et al.</i> (2019), Martin <i>et al.</i> (2014), da Silva <i>et al.</i> (2018), Hörbe and Hötzenendorfer (2015), Pattakou <i>et al.</i> (2018), Mashaly <i>et al.</i> (2022)

Table 4. Main Techniques, Methods, Processes, Frameworks, and Tools Used in the Literature

vulnerabilities are identified, the next step is deciding how to eliminate or mitigate them depending on the context; 3) Evaluation: Different designs or solutions are compared based on their effectiveness in reducing privacy risks; and 4) Iteration: The framework supports an iterative process, allowing for system re-evaluation to accommodate changes or new functionalities as they arise.

Privacy By Design (PbD) Privacy by Design (PbD) Cavoukian *et al.* (2021) is a method that integrates privacy as a foundational principle in the design and development of systems, processes, and products. PbD aims to ensure privacy is considered from the outset and throughout the entire project lifecycle rather than treating it as a secondary concern or an afterthought. PbD is built on seven fundamental principles Cavoukian *et al.* (2021): 1) Proactive, not reactive; preventative, not remedial; 2) Privacy as the default setting; 3) Privacy embedded into design; 4) Full functionality: positive-sum, not zero-sum; 5) End-to-end security: full lifecycle protection; 6) Visibility and transparency: keep it open; and 7) Respect for user privacy: keep it user-centric. In this context, Pattakou *et al.* (2018) analyzed existing privacy methodologies, examining how LINDDUN, SQUARE, and PriS align within the privacy framework by design. The study assessed the compliance of these frameworks and their support for PbD principles. The findings showed satisfactory results for the evaluated methodologies, confirming their compliance with PbD standards and their capability to support PbD.

Proposed Additional Techniques In addition to the techniques, methods, processes, frameworks, and tools previously presented, other studies have used one or more techniques: **1) KAOS (Method)** (Mouratidis *et al.* (2012), Huth and Matthes (2019), Ganji *et al.* (2015), Peixoto

et al. (2023), Kavakli *et al.* (2007), Pattakou *et al.* (2017), Peixoto *et al.* (2020)); **2) Goal-Based Requirements Analysis Method (GBRAM) (Method)** (Sangaroonsilp *et al.* (2023b), Mouratidis *et al.* (2012), Huth and Matthes (2019), Ganji *et al.* (2015), Kavakli *et al.* (2007), Ferrão *et al.* (2024)); **3) Role-Based Access Control (RBAC) (Technique)** (Mouratidis *et al.* (2012), Huth and Matthes (2019), Ganji *et al.* (2015), Krishnan and Vorobyov (2015), Pattakou *et al.* (2018)); **4) STRIDE (Framework)** (Deng *et al.* (2011), Veseli *et al.* (2019)); **5) PRIPARE (Method)** (Veseli *et al.* (2019), Herwanto *et al.* (2024d)); **6) P-STORE (Method)** (Herwanto *et al.* (2024d), Ansari *et al.* (2021)); **7) ISO 29100 (Framework)** (Freund *et al.* (2023), Martin *et al.* (2014), Ayala-Rivera and Pasquale (2018), Ferrão *et al.* (2024)); **8) Bellotti-Sellen Framework (Framework)** (Mouratidis *et al.* (2012), Kavakli *et al.* (2007), Jensen *et al.* (2005)); **9) Moffett-Nuseibeh Framework (M-N) (Framework)** (Mouratidis *et al.* (2012), Ganji *et al.* (2015), Kavakli *et al.* (2007)); **10) SecTro (Tool)** (Alkubaisy *et al.* (2021a), Diamantopoulou *et al.* (2018), Salnitri *et al.* (2020), Alkubaisy *et al.* (2021b)); **11) Privacy Criteria Method (PCM) (Method)** (Peixoto *et al.* (2023), Peixoto *et al.* (2019), Dias Canedo *et al.* (2020), Peixoto *et al.* (2024)); **12) ConflS (Framework)** (Alkubaisy *et al.* (2021a), Alkubaisy *et al.* (2021b)); **13) SepTA (Method)** (Salnitri *et al.* (2020), Alkubaisy *et al.* (2021b)); **14) Privacy Impact Assessment (PIA) (Method)** (Manna *et al.* (2022), Herwanto *et al.* (2024d), Ahmadian *et al.* (2019), Gopi *et al.* (2024), Makri *et al.* (2020)); **15) Asia-Pacific Economic Cooperation (APEC) Privacy Framework (Framework)** (Sangaroonsilp *et al.* (2023b), Sangaroonsilp *et al.* (2023a), Gopi *et al.* (2024)); **16) Non-Functional Requirement Framework (NFR) (Framework)** (Mouratidis *et al.* (2012), Huth and Matthes (2019), Ganji *et al.* (2015), Stach and Mitschang (2019), Peixoto *et al.* (2023), Peixoto and Silva (2018), de Sá Sousa *et al.* (2023), Shah and Patel

(2023)); **17) OECD Privacy Statement Generator (Tool)** (Miyazaki *et al.* (2008), Mead *et al.* (2011)); and **18) NIST (Framework)** (Roberts *et al.* (2023), Gopi *et al.* (2024), Silva and Sarkis (2023)).

Additionally, Peixoto *et al.* (2020) presented a catalog of privacy-related concepts, which includes I* (I-Star), Tropos, Problem Frames, NFR Framework, SI* Framework, GRL, Threat Model, Use Case Maps, SecBPMN-ml, UML4PF, Data Flow Diagrams, KAOS, Goal/Agent Modeling, Secure Tropos, Misuse Cases, UMLsec, UML, STS-ml, Legal GRL, CORAS Risk Modeling, User Requirements Notation, BPMN, Security-Aware Tropos, and Threat Tree. Finally, it is important to note that many of the primary studies identified in the SLR propose a framework or model that can serve as a tool in the requirements engineering stages to address privacy requirements, as shown in Table 5.

RQ.1 Summary: According to the literature, the most commonly used techniques, methods, processes, frameworks, and tools are: SQUARE, Secure Tropos, PriS, I* (I-Star), LINDDUN, STRAP, and Privacy by Design.

4.2 RQ.2. How are the techniques, methods, processes, frameworks, and tools identified in the literature and industry used in the phases of requirements engineering for privacy?

Of the 125 primary studies selected, 48 focused on specific stages of requirements engineering, as shown in Figure 5. Most studies concentrated on the requirements elicitation phase and proposed frameworks or models to address privacy requirements. Table 6 presents all the studies along with the respective phases of Requirements Engineering that they address.

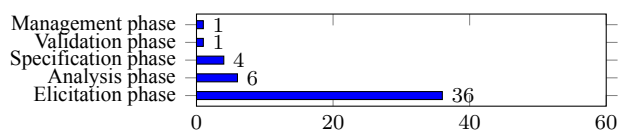


Figure 5. Number of Studies by Requirements Engineering Phase

Management: Stary and Heininger (2022) introduced a requirements management tool designed to support Cyber-Physical Systems (CPS) to enhance user control and transparency in managing privacy requirements. This tool enables the automated execution of behavior models and validates the model's behavior during runtime. It facilitates privacy management by promoting transparent autonomy sharing among the CPS components.

Elicitation: The studies Gharib *et al.* (2020) and Gharib *et al.* (2021) presented the development of the COPri and COPri v.2 ontologies, which aim to support the requirements elicitation phase for privacy. These studies focused on creating and refining an ontology to address the issue of requirements engineers' lack of understanding regarding specific privacy needs, distinguishing them from other types of re-

quirements, such as security. The ontology provides a comprehensive and expressive set of key concepts and relationships related to privacy, including consent from data subjects, as well as risk assessment and management of privacy threats, such as anonymization and data minimization.

Validation: Bijwe and Mead (2010) utilized the SQUARE process to validate the privacy requirements necessary for a software application. **Specification:** Deng *et al.* (2011) and Veseli *et al.* (2019) employed the LINDDUN framework to specify privacy requirements and presented potential privacy threats categorized into the seven LINDDUN categories, thereby facilitating the process of specifying privacy requirements. **Analysis:** Sahnitri *et al.* (2020) proposed a tool for modeling and analyzing requirements, including privacy requirements, security requirements, and trust requirements, aimed at minimizing the efforts of software developers in understanding these requirements.

RQ.2 Summary: Most studies utilized techniques, methods, processes, frameworks, and tools during the requirements elicitation phase, while few studies focused on the management, validation, and specification stages.

4.3 RQ.3 What are the challenges in eliciting privacy requirements?

Most studies selected in the SLR reported difficulties/challenges in eliciting privacy requirements. However, a pattern emerged in the problems mentioned, both in the elicitation of privacy requirements and in their practical implementation. The main problems and challenges identified were: 1) an increase in the complexity of software development, particularly during the requirements engineering phase, and 2) a direct conflict with security requirements, where, in some cases, team members cannot distinguish between security requirements and privacy requirements.

4.3.1 Increase in Software Development Complexity

Most studies indicated that the primary challenge in eliciting privacy requirements during the requirements engineering phase was the increased complexity of activities involved in this stage. This complexity arises from various factors, such as the difficulty requirements analysts/engineers and stakeholders have in understanding privacy requirements and how to apply them in practice, as well as the challenges in comprehending existing data privacy regulations and standards.

Sangaroonsilp *et al.* (2023b), Beckers and Heisel (2012), Manna *et al.* (2022), Kalloniatis *et al.* (2013), Thapa and Camtepe (2021), and Zhao *et al.* (2024), mentioned that one of the factors contributing to the increased complexity of software development is related to the difficulties in understanding and knowledge of privacy requirements. The authors emphasized that there is an additional burden of knowledge regarding privacy laws for developers when dealing with these requirements. Furthermore, they noted that there is often lower engagement from team members in addressing issues related to privacy requirements, either due to the complexity

Framework/Model Scope	References
Privacy Requirements in IoT	He <i>et al.</i> (2019) He <i>et al.</i> (2019), Stach and Mitschang (2019)
Privacy Concepts	Beckers and Heisel (2012), Manna <i>et al.</i> (2022), Olukoya (2022), Salnitri <i>et al.</i> (2020), Santana <i>et al.</i> (2022)
Privacy Threat and Requirements Analysis	Deng <i>et al.</i> (2011), Alkubaisy <i>et al.</i> (2021a), Sindre and Opdahl (2005), Zimmermann (2016), Salnitri <i>et al.</i> (2020), Ahmadian <i>et al.</i> (2019), Savola (2010), Sheth <i>et al.</i> (2014), Huang <i>et al.</i> (2023), Gopi <i>et al.</i> (2024)
Privacy Requirements Elicitation	Mouratidis <i>et al.</i> (2020), Argyropoulos <i>et al.</i> (2017), Sangaroonsilp <i>et al.</i> (2023b), Miyazaki <i>et al.</i> (2008), Roberts <i>et al.</i> (2023), Freund <i>et al.</i> (2023), Breaux <i>et al.</i> (2014), Martin <i>et al.</i> (2014), Peixoto <i>et al.</i> (2023), Kalloniatis <i>et al.</i> (2013), Herwanto <i>et al.</i> (2024d), Mai <i>et al.</i> (2018), Peixoto <i>et al.</i> (2019), Dias Canedo <i>et al.</i> (2020), Thapa and Camepe (2021) Radics <i>et al.</i> (2013), Stary and Heininger (2022), Gharib <i>et al.</i> (2016), Kavakli <i>et al.</i> (2007), Peixoto and Silva (2018), Diamantopoulou <i>et al.</i> (2017), Coles <i>et al.</i> (2018), Islam <i>et al.</i> (2010), Piras <i>et al.</i> (2020), Belhajjame <i>et al.</i> (2020), Kanwal <i>et al.</i> (2021), Rafiei and van der Aalst (2021), Herwanto <i>et al.</i> (2024b), Liang <i>et al.</i> (2020), Herwanto <i>et al.</i> (2024c), McDonald and Forte (2020), Herwanto <i>et al.</i> (2022), Shah and Patel (2023), Benthall and Cummings (2024), Peixoto <i>et al.</i> (2024), Terra <i>et al.</i> (2022), Vieira <i>et al.</i> (2023), de Jesus <i>et al.</i> (2024), Herwanto <i>et al.</i> (2024a), Gramajo <i>et al.</i> (2020), Ferrao and Canedo (2022)
Privacy Requirements for Smart Toys	Hung <i>et al.</i> (2016)
Security and Privacy Requirements Alignment	Mouratidis <i>et al.</i> (2012), Islam <i>et al.</i> (2015), Beckers (2012), Alkubaisy <i>et al.</i> (2019), Omitola <i>et al.</i> (2022), Makri <i>et al.</i> (2020), Anish <i>et al.</i> (2024), Alkubaisy <i>et al.</i> (2021b)
PriS	Kalloniatis <i>et al.</i> (2008), Kalloniatis <i>et al.</i> (2012), Kalloniatis <i>et al.</i> (2005), Kavakli <i>et al.</i> (2006), Kalloniatis <i>et al.</i> (2009), Kalloniatis <i>et al.</i> (2007)
COPri	Gharib <i>et al.</i> (2020), Gharib <i>et al.</i> (2021)
Privacy By Design, RBAC, PRET, P-STORE, Privacy-Enhanced BPMN (PE-BPMN), EPICUREAN, Secure Tropos, STRAP, TrUStAPIS	Perera <i>et al.</i> (2020), Krishnan and Vorobyov (2015), Mead <i>et al.</i> (2011), Ansari <i>et al.</i> (2021), Pullonen <i>et al.</i> (2019), Stach and Steimle (2019), Mouratidis and Giorgini (2007), Jensen <i>et al.</i> (2005), Ferraris and Gago (2020)
Privacy Legislation Compliance	Gjermundrød <i>et al.</i> (2016), Ayala-Rivera and Pasquale (2018), Ferrão <i>et al.</i> (2024), Bondel <i>et al.</i> (2020a), Zinsmaier <i>et al.</i> (2020), Diamantopoulou <i>et al.</i> (2020), Anwar and Gill (2021), Campanile <i>et al.</i> (2022), Mashaly <i>et al.</i> (2022), Amaral <i>et al.</i> (2023), Santos <i>et al.</i> (2024), Valença <i>et al.</i> (2022), de Sá Sousa <i>et al.</i> (2023), Alves and Neves (2021)
Privacy Requirements in Blockchain	Aslam <i>et al.</i> (2021)
Privacy Requirements in the Metaverse	Kang <i>et al.</i> (2023)

Table 5. Frameworks/Models Found

RE Phase	Reference
Elicitation	Kalloniatis <i>et al.</i> (2005), Kavakli <i>et al.</i> (2006), Kalloniatis <i>et al.</i> (2007), Kalloniatis <i>et al.</i> (2008), Miyazaki <i>et al.</i> (2008), Mead <i>et al.</i> (2011), Beckers and Heisel (2012), Mouratidis <i>et al.</i> (2012), Kalloniatis <i>et al.</i> (2012), Kalloniatis <i>et al.</i> (2013), Ganji <i>et al.</i> (2015), Anthonyamy <i>et al.</i> (2017), Pattakou <i>et al.</i> (2017), Diamantopoulou <i>et al.</i> (2017), Islam <i>et al.</i> (2015), Silva <i>et al.</i> (2018), da Silva <i>et al.</i> (2018), Huth and Matthes (2019), Röscher <i>et al.</i> (2019), Ahmadian <i>et al.</i> (2019), Stach and Steimle (2019), Alkubaisy <i>et al.</i> (2019), Gharib <i>et al.</i> (2020), Peixoto <i>et al.</i> (2020), Ferraris and Gago (2020), Alkubaisy <i>et al.</i> (2021a), Gharib <i>et al.</i> (2021), Ansari <i>et al.</i> (2021), Peixoto <i>et al.</i> (2023), Sangaroonsilp <i>et al.</i> (2023b), Sangaroonsilp <i>et al.</i> (2023a), Freund <i>et al.</i> (2023), Herwanto <i>et al.</i> (2024d), Zhao <i>et al.</i> (2024), Ferrão <i>et al.</i> (2024), Anish <i>et al.</i> (2024)
Analysis	Jensen <i>et al.</i> (2005), Kavakli <i>et al.</i> (2007), Spiekermann and Cranor (2008), Savola (2010), Salnitri <i>et al.</i> (2020), Pullonen <i>et al.</i> (2019)
Specification	Hörbe and Hötendorfer (2015), Gjermundrød <i>et al.</i> (2016), Veseli <i>et al.</i> (2019), Peixoto <i>et al.</i> (2019)
Validation	Bijwe and Mead (2010)
Management	Stary and Heininger (2022)

Table 6. Studies Related to Requirements Engineering Phases

of the privacy requirements themselves or the lack of appropriate tools to manage them.

Canedo *et al.* (2021a) and Herwanto *et al.* (2024d) also highlighted that privacy requirements elicitation could compromise the agility of the development process. Canedo *et al.* (2021a) investigated the challenges faced by agile software teams in addressing privacy requirements and suggested that development teams utilize checklists with simple language to discuss and present privacy requirements to stakeholders. This approach may help mitigate the negative impact on the team's agility. Additionally, Herwanto *et al.* (2024d) recommended that agile teams use automated tools to review privacy requirements.

Miyazaki *et al.* (2008) emphasized the need for an efficient methodology during the requirements engineering (RE) phase to address privacy requirements, as managing these requirements is complex given the time constraints of RE activ-

ities. This process also demands practitioners to be familiar with data privacy laws and the techniques necessary to ensure privacy. Similarly, Ganji *et al.* (2015) and Ferrão *et al.* (2024) reported on the difficulty practitioners face in handling the complex concepts found in privacy legislation and policies. Additionally, Martin *et al.* (2014) explored how privacy requirements can often appear vague and disconnected from the technology, further increasing the complexity and challenges of implementing these requirements in practice.

Given the various approaches available to handle privacy requirements, Spiekermann and Cranor (2008) discussed the importance of selecting the appropriate strategy to address privacy requirements across different contexts. The authors emphasized the need to carefully choose between approaches such as "privacy-by-policy" and "privacy-by-architecture," as selecting the wrong privacy practices can lead to additional development costs and unnecessary complexities.

Ayala-Rivera and Pasquale (2018) also addressed the challenge of choosing the best approach for managing privacy requirements and suggested that stakeholders thoroughly analyze the pros and cons of different data privacy strategies presented by the software development teams.

Casillo *et al.* (2022) and Sangaroonilp *et al.* (2023a) recommended that development teams explore the possibility of automating the requirements elicitation process by applying natural language processing (NLP) techniques. This approach could help identify not only privacy requirements but also security requirements. Additionally, Anthonysamy *et al.* (2017) suggested developing new privacy requirements models, emphasizing the need for a more in-depth perspective on privacy, considering complex concepts such as location privacy and probabilistically derived attributes.

4.3.2 Privacy Requirements vs. Security Requirements

Deng *et al.* (2011), Mouratidis *et al.* (2020), Argyropoulos *et al.* (2017), Mouratidis *et al.* (2012), Gharib *et al.* (2021), Alkubaisy *et al.* (2019), and Alkubaisy *et al.* (2019) reported difficulties in integrating privacy and security requirements. Although both aim primarily at data protection, their fundamental concepts often diverge and sometimes conflict during the requirements engineering phase. While most studies merely highlighted these challenges and suggested future research to address conflicts, some, such as Mouratidis *et al.* (2012) and Alkubaisy *et al.* (2019), proposed approaches to mitigate and resolve conflicts between privacy and security requirements.

Alkubaisy *et al.* (2019) highlighted the challenges and conflicts between privacy and security requirements, particularly emphasizing the requirements of Anonymity and Unobservability (privacy requirements that allow entities to use resources without revealing their identities). The authors noted that these requirements often conflict with security requirements, especially Accountability and Auditability (which require activity tracking and the linkage of actions to specific entities). To address these and other conflicts, the authors proposed identifying tools capable of simultaneously supporting privacy and security requirements. They emphasized the importance of evaluating these tools in various contexts to optimize their utility and performance.

Mouratidis *et al.* (2012) emphasized the need for an automated framework to support software development teams in modeling the relationship between privacy and security requirements. They presented the initial development of a framework designed to assist developers in eliciting privacy and security requirements in the early stages of the software development process.

Although other studies highlight conflicting aspects between privacy and security requirements, Bondel *et al.* (2020b) presented a perspective in which these requirements partially overlap, despite not being identical. The study offers two main interpretations: the first considers privacy as a subset of security, given that some security measures directly protect privacy. The second interpretation views these two concepts as parallel and serving distinct purposes, where security focuses on the technical and organizational resilience of systems, while privacy pertains to the ethical and legiti-

mate use of personal information.

4.3.3 Other Challenges

Some studies mentioned challenges in specific contexts that, while not representing a widespread issue, such as the increasing complexity in requirements engineering and software development phases, still pose significant problems within their respective fields of knowledge.

Huth and Matthes (2019) emphasized the need for conceptual models to aid in understanding the privacy concepts outlined by the General Data Protection Regulation (GDPR) Parliament and Council (2018), as the definition of privacy in the legislation contributes to confusion regarding what measures must be taken to ensure the privacy of user data. Similarly, Coles *et al.* (2018) highlighted the challenges in interpreting the principles of the GDPR, which can lead to ambiguity in how privacy requirements can be integrated into requirements engineering, potentially resulting in issues related to compliance with the law. As a partial solution to this problem, Rösch *et al.* (2019) presented 13 privacy control patterns that offer problem-oriented and pattern-based solutions for the technical requirements outlined by the GDPR Parliament and Council (2018). Additionally, the study by Tsohou *et al.* (2020) identified and consolidated 393 requirements encompassing legal aspects of privacy, security, and technology acceptance.

Still in the context of the GDPR, Schlehahn and Wenning (2018) presented a compliance tutorial on the transparency requirements of the regulation, along with an explanation of its data privacy vocabulary, facilitating adherence to the legislation. Regarding the Brazilian General Data Protection Law (LGPD) Brasil (2018), de Melo *et al.* (2024) highlighted the need for broader dissemination of information about the LGPD, both in terms of outreach and content volume. This is important for fostering a strong privacy culture, a need also emphasized in their study. The authors underscored the importance of implementing this culture to improve the handling of personal data, raise user awareness, and ensure corporate compliance.

RQ.3 Summary: The main challenges in addressing privacy requirements during Requirements Engineering are centered around two key issues. First, the increased complexity of software development when incorporating privacy concerns, which arises from difficulties in interpreting legal frameworks, low engagement from teams, and the lack of adequate tools and training. Second, the persistent confusion between privacy and security requirements, which often leads to misclassifications, conflicting priorities, and the use of inadequate methods.

5 Survey

We also conducted a survey to understand whether the techniques, methods, processes, frameworks, and tools in Requirements Engineering (RE) commonly described in the lit-

erature for the elicitation, analysis, specification, validation, and management of privacy requirements are known to or utilized by practitioners. We used the Google Forms platform to create the survey questionnaire. Three authors developed the survey questions, while the remaining authors validated them. We have conducted a pilot test round to evaluate the survey quality. We sent the questionnaire to three practitioners who work in the privacy area. Their feedback included suggestions regarding the questions' wording, deletion of repeated questions, changing some time intervals, and changing/including some answer options. We followed their advice and improved the questionnaire. The pilot respondents took about 10 minutes to complete the questionnaire. This time was reported when the survey questionnaire was made public.

The survey consisted of 16 questions: 15 closed-ended and 1 open-ended. At the beginning of the survey, we included an informed consent statement outlining the terms and conditions. The survey was anonymous, and no contact information was requested from respondents. We then made the survey available on various social media platforms, including LinkedIn, Facebook, and Instagram. The questionnaire was open from November 1st to November 28th, 2024, for a total of 28 days. In total, 37 practitioners responded to the survey. All questions and response options are available on Zenodo (Survey Questions). The majority of participants are from the Midwest region (32 participants) and have over 4 years of experience in software development (21 participants), working as programmers/developers. Table 7 presents the participants' profiles.

Seventy percent (70.3%) of participants reported that they have worked or are currently working on developing software features that involve data privacy concerns. However, 29.7% of participants stated that they have not (Q7). There were also 89.2% of participants who "strongly agree" or "agree" that their organization has implemented or is in the process of implementing changes due to the Brazilian General Data Protection Law (LGPD) (Q8). Additionally, 72.9% stated that their knowledge of the LGPD, which was enacted in 2020, is sufficient for carrying out their activities in the projects they are involved in. However, 16.2% reported that they lack the necessary knowledge to implement the LGPD (Q9) (Figure 6).

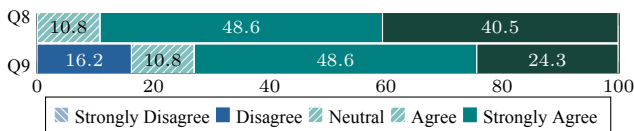


Figure 6. Practitioners' perceptions regarding how their organization has adapted to the LGPD (Q8) and their individual understanding of the law's requirements in the context of their daily project activities (Q9).

We also investigated which principles of the LGPD the participants were familiar with (Q10). The most well-known principles are security, data quality, transparency, and purpose, as shown in Figure 7. This finding is similar to the one identified in Canedo *et al.* (2021a) and Canedo *et al.* (2023), where participants in the study also reported being more familiar with these principles. Regarding the LGPD principles that participants' organizations use or implement

Region	#	%
Southeast	3	8.1
Midwest	33	89.2
South	1	2.7
Age group	#	%
21 to 25 years old	11	29.7
26 to 30 years old	4	10.8
31 to 36 years old	2	5.4
37 to 42 years old	5	13.5
43 to 47 years old	7	18.9
48 to 54 years old	6	16.2
61 years or more	2	5.4
Educational Level	#	%
Undergraduate student	7	18.9
Graduated	4	10.8
Postgraduate	5	13.5
Master student	12	32.4
Master	3	8.1
PhD student	4	10.8
PhD	2	5.4
Experience	#	%
>=1 years	4	10.8
Between 1 and 3 years	5	13.5
Between 4 and 6 years	7	18.9
Between 7 and 10 years	2	5.4
Between 11 and 15 years	3	8.1
Between 16 and 20 years	6	16.2
More than 21 years	10	27
Organization	#	%
Federal public administration	17	45.9
State public administration	7	18.9
Private software development company	10	27
Collaboration/Research Projects	3	8.1
Role	#	%
Programmer/Developer	25	67.5
Requirements Engineer	3	8.1
Data Protection Officer (DPO)	4	10.8
Other	5	13.51

Table 7. Demographics of the survey respondents (n= 37).

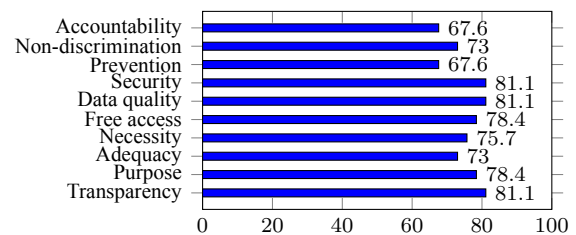


Figure 7. Principles of the LGPD known by practitioners

(Q11), practitioners stated that the most commonly used and implemented principles in their organizations are: Security (86.5%), Data Quality (75.7%), Purpose (75.5%), and Transparency (67.6%). Canedo *et al.* (2021a) also identified that the principles of security and purpose were the most implemented by practitioners.

Regarding the techniques, methods, processes, frameworks, and tools that practitioners have worked with or currently work with (Q12), only 10 participants reported having worked with Privacy by Design, and of those, only a few mentioned having worked with ISO 29100 and SQUARE. Therefore, the majority of practitioners do not use the techniques identified in the literature. Interestingly, our findings differ

from those of Canedo *et al.* (2023), where several practitioners reported using Pris, NFR, RBAC, PbD, PCM, and PET.

Regarding which phase of Requirements Engineering practitioners use techniques, methods, processes, frameworks, and tools to address privacy requirements, most of them reported that it is during the requirements analysis phase (56.8%) and specification phase (45.9%).

Regarding the tools used by the software development team to elicit and document privacy requirements (Q14), most participants reported not using any tools. However, 4 participants stated that they use SMaRT, and 2 participants reported using PRIS, Strap, and SPARQL, respectively. This finding is similar to the findings of Canedo *et al.* (2022).

Regarding the challenges practitioners face in eliciting privacy requirements, #P19 said: “Privacy laws may change, and it is essential that privacy requirements are always aligned with the most current regulations. Additionally, in context-sensitive systems (such as IoT), the collection and use of data increases the need for specific privacy requirements, as these systems often have to handle sensitive personal information.”; and #P28 said: “The absence of a dedicated team to address data privacy issues is the biggest challenge faced by my team”.

6 Discussions

The survey conducted with 37 practitioners provided valuable insights into how privacy requirements are approached in industrial contexts and allowed for a comparison with the findings of our Systematic Literature Review (SLR). While the SLR identified a broad range of techniques, methods, processes, frameworks, and tools proposed in the literature (RQ1), such as SQUARE, Secure Tropos, PriS, LINDDUN, STRAP, and Privacy by Design, the survey revealed that these approaches are largely unknown or unused by practitioners in real-world settings.

Most survey participants demonstrated general awareness of privacy regulations, especially the LGPD. However, structured practices for eliciting, analyzing, and managing privacy requirements are still rarely adopted in practice. Informal communication, checklists, or ad hoc strategies are commonly used, in contrast to the methodical processes described in academic research. This suggests a significant gap between academic developments and industry application, particularly with respect to the use of formal tools and processes to support privacy-focused RE activities (RQ2).

Participants also highlighted several recurring challenges that align with those reported in the literature (RQ3), including difficulty translating legal and regulatory language into actionable system requirements, confusion between privacy and security requirements, and a general lack of organizational support or prioritization of privacy in early development phases. Moreover, limited access to training resources and practical guidance specific to privacy requirements further hinders the ability of professionals to apply the concepts and methods found in the literature.

While the SLR indicated that the requirements elicitation phase is the most addressed in privacy-related research, with relatively fewer studies focusing on validation, specifica-

tion, or management, the survey confirmed that elicitation is also the phase where privacy is most frequently considered in practice—albeit in an informal and unstructured manner. This partial alignment highlights that while the literature correctly identifies the phase of greatest emphasis, the practical means of implementation are still lacking or inaccessible for practitioners.

Finally, the survey reinforced that privacy is often seen as a compliance issue managed outside the scope of software development teams, which limits the integration of privacy concerns into the RE lifecycle. These findings illustrate a clear mismatch between the advancements in the academic field and the level of maturity in industry practices. This disconnect underscores the need for more accessible, usable, and industry-oriented approaches that support privacy-aware requirements engineering.

7 Threats to Validity

The threats to validity of this study can be categorized into four main types: construct, internal, external, and conclusion validity Wohlin *et al.* (2012). Regarding construct validity, the primary concern lies in the potential ambiguity of definitions for terms such as “privacy requirements” and “tools,” which can vary across different studies. Additionally, there is a risk that the inclusion and exclusion criteria may not adequately capture all relevant studies. To address these risks, straightforward definitions for acceptance and exclusion criteria were established, and peer reviews were conducted among researchers to ensure consistency in applying these criteria.

Regarding internal validity, a common threat observed in all systematic literature reviews is the risk of bias in the selection of studies, which can lead to subjective judgments by researchers during the data extraction process. By following the guidelines established by Keele *et al.* (2007), it was possible to implement a series of practices aimed at minimizing this threat. One such practice was selecting databases recommended by the guidelines for searching for studies. In addition to this factor, applying rigorous quality criteria also contributed to mitigating the risks mentioned above, both for the initially selected databases and those used in the manual search conducted after the first stage of this review.

Regarding external validity, the categorization of techniques, methods, and tools into subgroups may not capture the nuances between similar approaches or may overlap categories, complicating comparative analysis. This is particularly true since minor differences in methodology or application can lead to divergent results among tools, even when they are classified and categorized similarly. To address this issue, the extraction criteria were defined to ensure that different nuances, contexts, and details could be extracted for each analyzed study. This approach allows for a level of differentiation among studies and tools that address the same themes and contexts, enhancing the overall external validity of the findings by acknowledging the complexities and variations inherent in the data.

Regarding conclusion validity, the heterogeneity of the studies and the qualitative synthesis of results can introduce

subjectivity into interpretations. Additionally, the ongoing evolution of privacy regulations and technologies may affect the relevance of findings over time. To mitigate the threats presented in this context, a timeframe of up to 20 years for the acceptance of studies was established, with a greater emphasis on research from the last 10 years. This approach aims to identify techniques from the literature that remain relevant and are currently used as foundational references while also seeking innovative and contemporary methodologies. Furthermore, a detailed classification of the studies was undertaken to provide a synthesis of their results and a thorough review by three authors of this study of the protocol adopted to conduct the systematic literature review.

Finally, the main threats to the validity of the survey include: (1) Sampling bias, as the participants may not fully represent the diversity of organizations and levels of privacy maturity in Brazil; (2) Self-selection bias, since practitioners who are more engaged or familiar with the LGPD may have been more likely to respond to the survey; and (3) Limited generalizability, as the specific focus on privacy may restrict the applicability of the findings to other organizational or regional contexts.

8 Conclusion

In this study, we identified 125 primary studies that explore various techniques, methods, processes, frameworks, and tools employed in requirements engineering to address privacy requirements. Our review highlights that, while a diverse array of approaches exists, most of the research is concentrated within academic contexts, with limited evidence of practical, large-scale application in industry settings. Widely utilized approaches such as PriS Method, Secure Tropos, LINDDUN, i* (i-star), STRAP, Privacy by Design (PbD), and SQUARE are primarily focused on the elicitation phase of privacy requirements, indicating a significant emphasis on the initial stages of requirements engineering. However, the lack of research dedicated to later stages—such as analysis, documentation, validation, and management—points to an urgent need for further exploration to ensure comprehensive integration of privacy requirements throughout the software development lifecycle.

Additionally, this review identified several challenges in eliciting privacy requirements, including the increasing complexity of software development and the confusion between privacy and security requirements. These challenges highlight the necessity for integrated approaches that can effectively address the nuances of privacy in the context of evolving data protection regulations. Survey results further underscore these challenges, revealing that while many practitioners are familiar with LGPD principles and agree their organizations are adapting to the regulation, the adoption of structured privacy engineering practices remains limited. Informal methods and the absence of tools during privacy requirements elicitation are prevalent, reflecting the need for greater awareness, targeted training, and practical resources to bridge the gap between theoretical knowledge and real-world implementation.

Future research should aim to bridge the gaps identified by

investigating the scalability, adaptability, and effectiveness of these techniques, methods, processes, frameworks, and tools across various real-world software environments. Such efforts would enhance the robustness of privacy-preserving practices in the requirements engineering phase and contribute to the development of privacy-conscious software systems that meet regulatory standards and user expectations.

Acknowledgements

This study was financed in part by the Project No. 514/2023 – Call N° 10/2023 – FAPDF Learning Program, a strategic development initiative in the macro areas of Agro Learning, Bio Learning, Gov Learning, and Tech Learning. This study was partially financed by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior—Brasil (CAPES), Finance Code 001.

Authors' Contributions

Stefano Luppi Spósito: Conceptualization, Data curation, Investigation, Methodology, Validation, Writing (original draft, review, and editing). João Francisco Gomes Targino: Investigation, Data curation, Visualization, Writing (original draft, review and editing). Geovana Ramos Sousa Silva: Investigation, Data curation, Visualization, Writing (review and editing). Laerte Peotta: Investigation, Methodology, Validation, Visualization, Writing (original draft, review, and editing). Daniel de Paula Porto: Conceptualization, Methodology, Co-supervision, Validation, Writing (review and editing). Fábio Lúcio Lopes Mendonça: Conceptualization, Data curation, Investigation, Writing (original draft, review, and editing), Supervision, Project administration.

Edna Dias Canedo: Conceptualization, Data curation, Investigation, Writing (original draft, review, and editing), Supervision, Project administration. All authors read and approved the final manuscript.

Competing interests

The authors declare that they have no conflict of interest.

Availability of data and materials

The supporting data for this work is available at <https://zenodo.org/records/15185984>.

References

- Achimugu, P., Selamat, A., Ibrahim, R., and Mahrin, M. N. (2014). A systematic literature review of software requirements prioritization research. *Inf. Softw. Technol.*, 56(6):568–585. DOI: 10.1016/J.INFSOF.2014.02.001.
- Ahmadian, A. S., Strüder, D., and Jürjens, J. (2019). Privacy-enhanced system design modeling based on privacy features. In *Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing*, pages 1492–1499. DOI: 10.1145/3297280.3297431.
- Alkubaisy, D., Cox, K., and Mouratidis, H. (2019). Towards detecting and mitigating conflicts for privacy and security requirements. In *2019 13th International Conference on Research Challenges in Information Science (RCIS)*, pages 1–6. IEEE. DOI: 10.1109/rcis.2019.8876999.

- Alkubaisy, D., Piras, L., Al-Obeidallah, M. G., Cox, K., and Mouratidis, H. (2021a). Confis: a tool for privacy and security analysis and conflict resolution for supporting gdpr compliance through privacy-by-design. In *International Conference on Evaluation of Novel Approaches to Software Engineering, ENASE-Proceedings*, volume 2021, pages 80–91. SCITEPRESS-Science and Technology Publications. DOI: 10.5220/00104061008000091.
- Alkubaisy, D., Piras, L., Al-Obeidallah, M. G., Cox, K., and Mouratidis, H. (2021b). A framework for privacy and security requirements analysis and conflict resolution for supporting gdpr compliance through privacy-by-design. In *International Conference on Evaluation of Novel Approaches to Software Engineering*, pages 67–87. Springer. DOI: 10.1007/978-3-030-96648-5₄.
- Alves, C. and Neves, M. (2021). Especificação de requisitos de privacidade em conformidade com a lgpd: Resultados de um estudo de caso. In *WER*. Available at: http://wer.inf.puc-rio.br/WERpapers/artigos/artigos_WER21/WER_2021_paper_31.pdf.
- Amaral, O., Abualhaija, S., and Briand, L. (2023). ML-based compliance verification of data processing agreements against gdpr. In *2023 IEEE 31st international requirements engineering conference (RE)*, pages 53–64. IEEE. DOI: 10.1109/re57278.2023.00015.
- Anish, P. R., Verma, A., Venkatesan, S., V., L., and Ghaisas, S. (2024). Governance-focused classification of security and privacy requirements from obligations in software engineering contracts. In Mendez, D. and Moreira, A., editors, *Requirements Engineering: Foundation for Software Quality*, pages 92–108, Cham. Springer Nature Switzerland. DOI: 10.1007/978-3-031-57327-9₆.
- Ansari, M. T. J., Baz, A., Alhakami, H., Alhakami, W., Kumar, R., and Khan, R. A. (2021). P-store: Extension of store methodology to elicit privacy requirements. *Arabian Journal for Science and Engineering*, 46:8287–8310. DOI: 10.1007/s13369-021-05476-z.
- Anthonyamy, P., Rashid, A., and Chitchyan, R. (2017). Privacy requirements: present & future. In *2017 IEEE/ACM 39th international conference on software engineering: software engineering in society track (ICSE-SEIS)*, pages 13–22. IEEE. Book.
- Anwar, M. J. and Gill, A. (2021). Developing an integrated iso 27701 and gdpr based information privacy compliance requirements model. In *Australasian Conference on Information Systems 2020*. Available at: <https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1055&context=acis2020>.
- Argyropoulos, N., Shei, S., Kalloniatis, C., Mouratidis, H., Delaney, A. J., Fish, A., and Gritzalis, S. (2017). A semi-automatic approach for eliciting cloud security and privacy requirements. In Bui, T., editor, *50th Hawaii International Conference on System Sciences, HICSS 2017, Hilton Waikoloa Village, Hawaii, USA, January 4-7, 2017*, pages 1–10. ScholarSpace / AIS Electronic Library (AISeL). DOI: 10.24251/hicss.2017.587.
- Aslam, S., Tošić, A., and Mrissa, M. (2021). Secure and privacy-aware blockchain design: Requirements, challenges and solutions. *Journal of Cybersecurity and Privacy*, 1(1):164–194. DOI: 10.3390/jcp1010009.
- Ayala-Rivera, V. and Pasquale, L. (2018). The grace period has ended: An approach to operationalize gdpr requirements. In *2018 IEEE 26th International Requirements Engineering Conference (RE)*, pages 136–146. IEEE. DOI: 10.1109/re.2018.00023.
- Beckers, K. (2012). Comparing privacy requirements engineering approaches. In *2012 Seventh International Conference on Availability, Reliability and Security*, pages 574–581. IEEE. DOI: 10.1109/ares.2012.29.
- Beckers, K. and Heisel, M. (2012). A foundation for requirements analysis of privacy preserving software. In Quirchmayr, G., Basl, J., You, I., Xu, L., and Weippl, E., editors, *Multidisciplinary Research and Practice for Information Systems*, pages 93–107, Berlin, Heidelberg. Springer Berlin Heidelberg. DOI: 10.1007/978-3-642-32498-7₈.
- Belhajjame, K., Fati, N., Maamar, Z., Burégio, V., Soares, E., and Barhamgi, M. (2020). On privacy-aware escience workflows. *Computing*, 102:1171–1185. DOI: 10.1007/s00607-019-00783-8.
- Benthall, S. and Cummings, R. (2024). Integrating differential privacy and contextual integrity. In *Proceedings of the Symposium on Computer Science and Law*, pages 9–15. DOI: 10.1145/3614407.3643702.
- Bijwe, A. and Mead, N. R. (2010). Adapting the square process for privacy requirements engineering. *Software Engineering Institute: Pittsburgh, PA, USA*. DOI: 10.1184/R1/6571826.v1.
- Bondel, G., Garrido, G. M., Baumer, K., and Matthes, F. (2020a). Towards a privacy-enhancing tool based on de-identification methods. In Vogel, D., Shen, K. N., Ling, P. S., Hsu, C., Thong, J. Y. L., Marco, M. D., Limayem, M., and Xu, S. X., editors, *24th Pacific Asia Conference on Information Systems, PACIS 2020, Dubai, UAE, June 22-24, 2020*, page 157. Available at: <https://aisel.aisnet.org/pacis2020/157>.
- Bondel, G., Garrido, G. M., Baumer, K., and Matthes, F. (2020b). The use of de-identification methods for secure and privacy-enhancing big data analytics in cloud environments. In *ICEIS (2)*, pages 338–344.
- Brasil (2018). Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). *Diário Oficial da República Federativa do Brasil*. http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.
- Breaux, T. D., Hibshi, H., and Rao, A. (2014). Eddy, a formal language for specifying and analyzing data flow specifications for conflicting privacy requirements. *Requirements Engineering*, 19:281–307. DOI: 10.1007/s00766-013-0190-7.
- Caiza, J. C., Martín, Y. S., Guamán, D. S., del álamo, J. M., and Yelmo, J. C. (2019). Reusable elements for the systematic design of privacy-friendly information systems: A mapping study. *IEEE Access*, 7:66512–66535. DOI: 10.1109/ACCESS.2019.2918003.
- Campanile, L., Iacono, M., and Mastroianni, M. (2022). Towards privacy-aware software design in small and medium enterprises. In *2022 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive*

- Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Confor Cyber Science and Technology Congress (DASC/PiCom/CBDCOM/CyberSciTech)*, pages 1–8. IEEE. DOI: 10.1109/dasc/picom/cbdcom/cy55231.2022.9927958.
- Camêlo, M. N. and Alves, C. (2023). G-priv: Um guia para apoiar a especificação de requisitos de privacidade em conformidade com a LGPD. *Braz. J. Inf. Syst.*, 16(1). DOI: 10.5753/ISYS.2023.2743.
- Canedo, E. D., Bandeira, I. N., Calazans, A. T. S., Costa, P. H. T., Cançado, E. C. R., and Bonifácio, R. (2023). Privacy requirements elicitation: a systematic literature review and perception analysis of IT practitioners. *Requir. Eng.*, 28(2):177–194. DOI: 10.1007/S00766-022-00382-8.
- Canedo, E. D., Calazans, A. T. S., Bandeira, I. N., Costa, P. H. T., and Masson, E. T. S. (2022). Guidelines adopted by agile teams in privacy requirements elicitation after the brazilian general data protection law (LGPD) implementation. *Requir. Eng.*, 27(4):545–567. DOI: 10.1007/S00766-022-00391-7.
- Canedo, E. D., Calazans, A. T. S., Cerqueira, A. J., Costa, P. H. T., and Masson, E. T. S. (2020). Using the design thinking empathy phase as a facilitator in privacy requirements elicitation. In Anderson, B. B., Thatcher, J., Meservy, R. D., Chudoba, K., Fadel, K. J., and Brown, S., editors, *26th Americas Conference on Information Systems, AMCIS 2020, Virtual Conference, August 15-17, 2020*. Association for Information Systems. Available at: https://aisel.aisnet.org/amcis2020/info_security_privacy/info_security_privacy/27.
- Canedo, E. D., Calazans, A. T. S., Cerqueira, A. J., Costa, P. H. T., and Masson, E. T. S. (2021a). Agile teams’ perception in privacy requirements elicitation: Lgpd’s compliance in brazil. In *2021 IEEE 29th International Requirements Engineering Conference (RE)*, pages 58–69. IEEE. DOI: 10.1109/re51729.2021.00013.
- Canedo, E. D., Cerqueira, A. J., Gravina, R. M., Ribeiro, V. C., Camões, R., dos Reis, V. E., de Mendonça, F. L. L., and de Sousa Jr, R. T. (2021b). Proposal of an implementation process for the brazilian general data protection law (lgpd). In *ICEIS (I)*, pages 19–30. DOI: 10.5220/0010398200190030.
- Casillo, F., Deufemia, V., and Gravino, C. (2022). Detecting privacy requirements from user stories with nlp transfer learning models. *Information and Software Technology*, 146:106853. DOI: 10.1016/j.infsof.2022.106853.
- Castro, J., Kolp, M., and Mylopoulos, J. (2001). A requirements-driven development methodology. In *Advanced Information Systems Engineering: 13th International Conference, CAiSE 2001 Interlaken, Switzerland, June 4–8, 2001 Proceedings 13*, pages 108–123. Springer. DOI: 10.1007/3-540-45341-5_8.
- Cavoukian, A. et al. (2021). Privacy by design: The seven foundational principles. *IAPP Resource Center*. Available at: <https://iapp.org/resources/article/privacy-by-design-the-7-foundational-principles>.
- Cheung, M. Y. M. and Liu, H. (2023). Information privacy concerns in generative AI. In *Australasian Conference on Information Systems, ACIS 2023, Wellington, New Zealand, December 5-8, 2023*. Available at: <https://aisel.aisnet.org/acis2023/24>.
- Coles, J., Faily, S., and Ki-Aries, D. (2018). Tool-supporting data protection impact assessments with cairis. In *2018 IEEE 5th International Workshop on Evolving Security & Privacy Requirements Engineering (ESPRe)*, pages 21–27. IEEE. DOI: 10.1109/espre.2018.00010.
- da Silva, M., Viterbo, J., Bernardini, F., and Maciel, C. (2018). Identifying privacy functional requirements for crowdsourcing applications in smart cities. In *2018 IEEE International Conference on Intelligence and Security Informatics (ISI)*, pages 106–111. DOI: 10.1109/ISI.2018.8587316.
- de Jesus, E. D. B., Vilela, J., and Silva, C. (2024). Requisitos de segurança e privacidade em startups: Um estudo empírico em uma aplicação de governança de dados. In Lucena, M., Lencastre, M., and Ballejos, L. C., editors, *Anais do WER24 - Workshop em Engenharia de Requisitos, Buenos Aires, Argentina, August 7-9, 2024*. Even3, Brasil. DOI: 10.29327/1407529.27-13.
- de Melo, R. O. P., Vilela, J., and Silva, C. (2024). Do entendimento à aplicação: Requisitos de privacidade e a visão dos usuários sobre a LGPD. In Lucena, M., Lencastre, M., and Ballejos, L. C., editors, *Anais do WER24 - Workshop em Engenharia de Requisitos, Buenos Aires, Argentina, August 7-9, 2024*. Even3, Brasil. DOI: 10.29327/1407529.27-27.
- de Sá Sousa, H. P., Almentero, E. K., de Classe, T. M., dos Santos, R. J., and Leite, J. C. S. P. (2023). Uma abordagem baseada no catálogo de requisitos não funcionais para conformidade à lgpd. In *WER*. Available at: http://wer.inf.puc-rio.br/WERpapers/artigos/artigos_WER23/WER_2023_paper_39.pdf.
- Deng, M., Wuyts, K., Scandariato, R., Preneel, B., and Joosen, W. (2011). A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. *Requirements Engineering*, 16(1):3–32. DOI: 10.1007/s00766-010-0115-7.
- Diamantopoulou, V., Androutsopoulou, A., Gritzalis, S., and Charalabidis, Y. (2020). Preserving digital privacy in e-participation environments: Towards gdpr compliance.
- Diamantopoulou, V., Argyropoulos, N., Kalloniatis, C., and Gritzalis, S. (2017). Supporting the design of privacy-aware business processes via privacy process patterns. In *2017 11th International Conference on Research Challenges in Information Science (RCIS)*, pages 187–198. IEEE. DOI: 10.1109/rcis.2017.7956536.
- Diamantopoulou, V., Pavlidis, M., and Mouratidis, H. (2018). Evaluation of a security and privacy requirements methodology using the physics of notation. In *Computer Security: ESORICS 2017 International Workshops, CyberICPS 2017 and SECPRE 2017, Oslo, Norway, September 14-15, 2017, Revised Selected Papers 3*, pages 210–225. Springer. DOI: 10.1007/978-3-319-72817-9_14.
- Dias Canedo, E., Toffano Seidel Calazans, A., Toffano Seidel Masson, E., Teixeira Costa, P. H., and Lima, F. (2020). Perceptions of ict practitioners regarding software privacy.

- Entropy*, 22(4):429. DOI: 10.3390/e22040429.
- Ebrahimi, F., Tushev, M., and Mahmoud, A. (2021). Mobile app privacy in software engineering research: A systematic mapping study. *Information and Software Technology*, 133:106466. DOI: 10.1016/j.infsof.2020.106466.
- Ferrao, S. E. R. and Canedo, E. D. (2022). Uma taxonomia para requisitos de privacidade e sua aplicação no open banking brasil. In *WER*. Available at: http://wer.inf.puc-rio.br/WERpapers/artigos/artigos_WER22/WER_2022_Camera_ready_paper_14.pdf.
- Ferraris, D. and Gago, M. C. F. (2020). Trustapis: a trust requirements elicitation method for iot. *Int. J. Inf. Sec.*, 19(1):111–127. DOI: 10.1007/S10207-019-00438-X.
- Ferrão, S. □. R., Silva, G. R. S., Canedo, E. D., and Mendes, F. F. (2024). Towards a taxonomy of privacy requirements based on the lgpd and iso/iec 29100. *Information and Software Technology*, page 107396. DOI: 10.1016/j.infsof.2024.107396.
- Frej, M., Neto, I. P. G., Ferreira, W., and Soares, S. (2024). Um sistema web para auxiliar soluções na conformidade com a LGPD. In *Proceedings of the 38th Brazilian Symposium on Software Engineering, SBES 2024, Curitiba, Brazil, September 30 - October 4, 2024*, pages 713–719. DOI: 10.5753/SBES.2024.3558.
- Freund, G. P., Macedo, D. D. J. d., and Fagundes, P. B. (2023). Data protection and privacy: a model for evidence management. *Em Questão*, 29:e–128009. DOI: 10.1590/1808-5245.29.128009.
- Ganji, D., Mouratidis, H., Gheytaasi, S. M., and Petridis, M. (2015). Conflicts between security and privacy measures in software requirements engineering. In *Global Security, Safety and Sustainability: Tomorrow's Challenges of Cyber Security: 10th International Conference, ICGS3 2015, London, UK, September 15-17, 2015. Proceedings 10*, pages 323–334. Springer. DOI: 10.1007/978-3-319-23276-8_29.
- Gharib, M., Giorgini, P., and Mylopoulos, J. (2017). Towards an ontology for privacy requirements via a systematic literature review. In *Conceptual Modeling: 36th International Conference, ER 2017, Valencia, Spain, November 6–9, 2017, Proceedings 36*, pages 193–208. Springer. DOI: 10.1007/978-3-319-69904-2_16.
- Gharib, M., Giorgini, P., and Mylopoulos, J. (2021). Copri v. 2—a core ontology for privacy requirements. *Data & Knowledge Engineering*, 133:101888. DOI: 10.1016/j.datak.2021.101888.
- Gharib, M., Mylopoulos, J., and Giorgini, P. (2020). Copri: a core ontology for privacy requirements engineering. In *Research Challenges in Information Science: 14th International Conference, RCIS 2020, Limassol, Cyprus, September 23–25, 2020, Proceedings 14*, pages 472–489. Springer. Book.
- Gharib, M., Salnitri, M., Paja, E., Giorgini, P., Mouratidis, H., Pavlidis, M., Ruiz, J. F., Fernandez, S., and Della Siria, A. (2016). Privacy requirements: findings and lessons learned in developing a privacy platform. In *2016 IEEE 24th International Requirements Engineering Conference (RE)*, pages 256–265. IEEE. DOI: 10.1109/re.2016.13.
- Gjermundrød, H., Dionysiou, I., and Costa, K. (2016). privacytracker: a privacy-by-design gdpr-compliant framework with verifiable data traceability controls. In *Current Trends in Web Engineering: ICWE 2016 International Workshops, DUI, TELERISE, SoWeMine, and Liquid Web, Lugano, Switzerland, June 6–9, 2016. Revised Selected Papers 16*, pages 3–15. Springer. DOI: 10.1007/978-3-319-46963-8_1.
- Golda, A., Mekonen, K., Pandey, A., Singh, A., Hassija, V., Chamola, V., and Sikdar, B. (2024). Privacy and security concerns in generative AI: A comprehensive survey. *IEEE Access*, 12:48126–48144. DOI: 10.1109/ACCESS.2024.3381611.
- Gopi, G., Maddi, A., Arasaratnam, O., and Fanti, G. (2024). Privacy requirements and realities of digital public goods. In *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)*, pages 159–177. DOI: 10.48550/arxiv.2406.15842.
- Gramajo, M. G., Ballejos, L. C., and Ale, M. (2020). Hacia la evaluación automática de la calidad de los requerimientos de software usando redes neuronales long short term memory. In *WER*. Available at: http://wer.inf.puc-rio.br/WERpapers/artigos/artigos_WER20/05_WER_2020_paper_33.pdf.
- Hansen, M., Jensen, M., and Rost, M. (2015). Protection goals for privacy engineering. In *2015 IEEE Symposium on Security and Privacy Workshops, SPW 2015, San Jose, CA, USA, May 21–22, 2015*, pages 159–166. IEEE Computer Society. DOI: 10.1109/SPW.2015.13.
- He, Y., Bahirat, P., Knijnenburg, B. P., and Menon, A. (2019). A data-driven approach to designing for privacy in household iot. *ACM Trans. Interact. Intell. Syst.*, 10(1). DOI: 10.1145/3241378.
- Herwanto, G. B., Ekaputra, F. J., Quirchmayr, G., and Tjoa, A. M. (2024a). Towards a holistic privacy requirements engineering process: Insights from a systematic literature review. *IEEE Access*. DOI: 10.1109/ACCESS.2024.3380888.
- Herwanto, G. B., Putri, D. U. K., Ningtyas, A. M., Fuad, A., Quirchmayr, G., and Tjoa, A. M. (2024b). Integrating contextual integrity in privacy requirements engineering: A study case in personal e-health applications. In *International Conference on Innovations for Community Services*, pages 237–256. Springer. DOI: 10.1007/978-3-031-60433-1_14.
- Herwanto, G. B., Quirchmayr, G., and Tjoa, A. M. (2022). From user stories to data flow diagrams for privacy awareness: A research preview. In *International Working Conference on Requirements Engineering: Foundation for Software Quality*, pages 148–155. Springer. DOI: 10.1007/978-3-030-98464-9_12.
- Herwanto, G. B., Quirchmayr, G., and Tjoa, A. M. (2024c). Learning to rank privacy design patterns: A semantic approach to meeting privacy requirements. In Mendez, D. and Moreira, A., editors, *Requirements Engineering: Foundation for Software Quality*, pages 57–73. Cham. Springer Nature Switzerland. DOI: 10.1007/978-3-031-57327-9_4.
- Herwanto, G. B., Quirchmayr, G., and Tjoa, A. M. (2024d). Leveraging nlp techniques for privacy requirements engi-

- neering in user stories. *IEEE Access*. DOI: 10.1109/access.2024.3364533.
- Hidellaarachchi, D., Grundy, J., Hoda, R., and Madampe, K. (2021). The effects of human aspects on the requirements engineering process: A systematic literature review. *IEEE Transactions on Software Engineering*, 48(6):2105–2127. DOI: 10.1109/tse.2021.3051898.
- Huang, T., Kaulagi, V., Hosseini, M. B., and Breau, T. (2023). Mobile application privacy risk assessments from user-authored scenarios. In *2023 IEEE 31st International Requirements Engineering Conference (RE)*, pages 17–28. IEEE. DOI: 10.1109/re57278.2023.00012.
- Hung, P. C. K., Fantinato, M., and Rafferty, L. (2016). A study of privacy requirements for smart toys. In Liang, T., Hung, S., Chau, P. Y. K., and Chang, S., editors, *20th Pacific Asia Conference on Information Systems, PACIS 2016, Chiayi, Taiwan, June 27 - July 1, 2016*, page 71. Available at: <http://aisel.aisnet.org/pacis2016/71>.
- Huth, D. and Matthes, F. (2019). "appropriate technical and organizational measures": Identifying privacy engineering approaches to meet GDPR requirements. In *25th Americas Conference on Information Systems, AMCIS 2019, Cancún, Mexico, August 15-17, 2019*. Association for Information Systems. Available at: https://aisel.aisnet.org/amcis2019/info_security_privacy/info_security_privacy/5.
- Hörbe, R. and Hötendorfer, W. (2015). Privacy by design in federated identity management. In *2015 IEEE Security and Privacy Workshops*, pages 167–174. IEEE. DOI: 10.1109/spw.2015.24.
- Islam, S., Mouratidis, H., and Wagner, S. (2010). Towards a framework to elicit and manage security and privacy requirements from laws and regulations. In *Requirements Engineering: Foundation for Software Quality: 16th International Working Conference, REFSQ 2010, Essen, Germany, June 30–July 2, 2010. Proceedings 16*, pages 255–261. Springer. DOI: 10.1007/978-3-642-14192-8_23.
- Islam, S., Ouedraogo, M., Kalloniatis, C., Mouratidis, H., and Gritzalis, S. (2015). Assurance of security and privacy requirements for cloud deployment models. *IEEE Transactions on Cloud Computing*, 6(2):387–400. DOI: 10.1109/tcc.2015.2511719.
- Jensen, C., Tullio, J., Potts, C., and Mynatt, E. D. (2005). Strap: a structured analysis framework for privacy. *Georgia Institute of Technology*, 1. Available at: <https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=a86cc96eed21f3a8237b84c9c3d792517c346b6b>.
- Kalloniatis, C., Belsis, P., Kavakli, E., and Gritzalis, S. (2012). Applying soft computing technologies for implementing privacy-aware systems. In *Advanced Information Systems Engineering Workshops: CAiSE 2012 International Workshops, Gdańsk, Poland, June 25-26, 2012. Proceedings 24*, pages 31–45. Springer. DOI: 10.1007/978-3-642-31069-0_3.
- Kalloniatis, C., Kavakli, E., and Gritzalis, S. (2005). Dealing with privacy issues during the system design process. In *Proceedings of the Fifth IEEE International Symposium on Signal Processing and Information Technology, 2005.*, pages 546–551. IEEE. DOI: 10.1109/ispit.2005.1577156.
- Kalloniatis, C., Kavakli, E., and Gritzalis, S. (2007). Using privacy process patterns for incorporating privacy requirements into the system design process. In *The Second International Conference on Availability, Reliability and Security (ARES'07)*, pages 1009–1017. IEEE. DOI: 10.1109/ares.2007.156.
- Kalloniatis, C., Kavakli, E., and Gritzalis, S. (2008). Addressing privacy requirements in system design: the pris method. *Requirements Engineering*, 13:241–255. DOI: 10.1007/s00766-008-0067-3.
- Kalloniatis, C., Kavakli, E., and Kontellis, E. (2009). Pris tool: A case tool for privacy-oriented requirements engineering. In Poullymenakou, A., Pouloudi, N., and Pramatari, K., editors, *The 4th Mediterranean Conference on Information Systems, MCIS 2009, Athens University of Economics and Business, AUEB, Athens, Greece, 25-27 September 2009*, page 71. Athens University of Economics and Business / AISel. Available at: <http://aisel.aisnet.org/mcis2009/71>.
- Kalloniatis, C., Mouratidis, H., and Islam, S. (2013). Evaluating cloud deployment scenarios based on security and privacy requirements. *Requirements Engineering*, 18:299–319. DOI: 10.1007/s00766-013-0166-7.
- Kang, G., Koo, J., and Kim, Y.-G. (2023). Security and privacy requirements for the metaverse: A metaverse applications perspective. *IEEE Communications Magazine*, 62(1):148–154. DOI: 10.1109/mcom.014.2200620.
- Kanwal, T., Anjum, A., and Khan, A. (2021). Privacy preservation in e-health cloud: taxonomy, privacy requirements, feasibility analysis, and opportunities. *Cluster Computing*, 24(1):293–317. DOI: 10.1007/s10586-020-03106-1.
- Kavakli, E., Gritzalis, S., and Christos, K. (2007). Protecting privacy in system design: the electronic voting case. *Transforming Government: People, Process and Policy*, 1(4):307–332. DOI: 10.1108/17506160710839150.
- Kavakli, E., Kalloniatis, C., Loucopoulos, P., and Gritzalis, S. (2006). Incorporating privacy requirements into the system design process: the pris conceptual framework. *Internet research*, 16(2):140–158. DOI: 10.1108/10662240610656483.
- Keele, S. et al. (2007). Guidelines for performing systematic literature reviews in software engineering. Available at: https://legacyfiles.elsevier.com/promis_misc/525444systematicreviewsguide.pdf.
- Krishnan, P. and Vorobyov, K. (2015). Enforcement of privacy requirements. *Computers & Security*, 52:164–177. DOI: 10.1016/j.cose.2015.03.004.
- Liang, W., Chen, H., Liu, R., Wu, Y., and Li, C. (2020). A pufferfish privacy mechanism for monitoring web browsing behavior under temporal correlations. *Computers & Security*, 92:101754. DOI: 10.1016/j.cose.2020.101754.
- Mai, P. X., Goknil, A., Shar, L. K., Pastore, F., Briand, L. C., and Shaame, S. (2018). Modeling security and privacy requirements: a use case-driven approach. *Information and Software Technology*, 100:165–182. DOI:

- 10.1016/j.infsof.2018.04.007.
- Makri, E.-L., Georgiopolou, Z., and Lambrinouidakis, C. (2020). Utilizing a privacy impact assessment method using metrics in the healthcare sector. *Information & Computer Security*, 28(4):503–529. DOI: 10.1108/ics-01-2020-0007.
- Manna, A., Sengupta, A., and Mazumdar, C. (2022). A risk-based methodology for privacy requirements elicitation and control selection. *SECURITY AND PRIVACY*, 5(1):e188. DOI: 10.1002/spy2.188.
- Martin, Y.-S., Del Alamo, J. M., and Yelmo, J. C. (2014). Engineering privacy requirements valuable lessons from another realm. In *2014 IEEE 1st International Workshop on Evolving Security and Privacy Requirements Engineering (ESPRe)*, pages 19–24. IEEE. DOI: 10.1109/espre.2014.6890523.
- Mashaly, B., Selim, S., Yousef, A. H., and Fouad, K. M. (2022). Privacy by design: A microservices-based software architecture approach. In *2022 2nd International Mobile, Intelligent, and Ubiquitous Computing Conference (MIUCC)*, pages 357–364. IEEE. DOI: 10.1109/miucc55081.2022.9781685.
- McDonald, N. and Forte, A. (2020). The politics of privacy theories: Moving from norms to vulnerabilities. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–14. DOI: 10.1145/3313831.3376167.
- Mead, N. R., Miyazaki, S., and Zhan, J. (2011). Integrating privacy requirements considerations into a security requirements engineering method and tool. *International Journal of Information Privacy, Security and Integrity*, 1(1):106–126. DOI: 10.1504/ijipsi.2011.043733.
- Miyazaki, S., Mead, N., and Zhan, J. (2008). Computer-aided privacy requirements elicitation technique. In *2008 IEEE Asia-Pacific Services Computing Conference*, pages 367–372. IEEE. DOI: 10.1109/apscc.2008.263.
- Mouratidis, H. and Giorgini, P. (2007). Secure tropos: a security-oriented extension of the tropos methodology. *International Journal of Software Engineering and Knowledge Engineering*, 17(02):285–309. DOI: 10.1142/s0218194007003240.
- Mouratidis, H., Kalloniatis, C., Islam, S., Huget, M.-P., and Gritzalis, S. (2012). Aligning security and privacy to support the development of secure information systems. *J. Univers. Comput. Sci.*, 18(12):1608–1627. DOI: 10.3217/jucs-018-12-1608.
- Mouratidis, H., Shei, S., and Delaney, A. (2020). A security requirements modelling language for cloud computing environments. *Software and Systems Modeling*, 19(2):271–295. DOI: 10.1007/s10270-019-00747-8.
- Notario, N., Crespo, A., Martín, Y. S., del Álamo, J. M., Métayer, D. L., Antignac, T., Kung, A., Kroener, I., and Wright, D. (2015). PRIPARE: integrating privacy best practices into a privacy engineering methodology. In *2015 IEEE Symposium on Security and Privacy Workshops, SPW 2015, San Jose, CA, USA, May 21–22, 2015*, pages 151–158. IEEE Computer Society. DOI: 10.1109/SPW.2015.22.
- Olukoya, O. (2022). Assessing frameworks for eliciting privacy & security requirements from laws and regulations. *Computers & Security*, 117:102697. DOI: 10.1016/j.cose.2022.102697.
- Omitola, T., Tsakalakis, N., Wills, G., Gomer, R., Waterson, B., Cherret, T., and Stalla-Bourdillon, S. (2022). User configurable privacy requirements elicitation in cyber-physical systems. In *Adjunct Proceedings of the 30th ACM Conference on User Modeling, Adaptation and Personalization*, pages 109–119. DOI: 10.1145/3511047.3537683.
- Parliament, T. E. and Council, T. (2018). General Data Protection Regulation (GDPR). *Intersoft Consulting*. Available at: <https://gdpr-info.eu>.
- Pattakou, A., Kalloniatis, C., and Gritzalis, S. (2017). Security and privacy requirements engineering methods for traditional and cloud-based systems: a review. *Cloud Comput.*, 2017:155. Available at: https://personales.upv.es/thinkmind/dl/conferences/cloudcomputing/cloud_computing_2017/cloud_computing_2017_8_10_28013.pdf.
- Pattakou, A., Mavroeidi, A.-G., Diamantopoulou, V., Kalloniatis, C., and Gritzalis, S. (2018). Towards the design of usable privacy by design methodologies. In *2018 IEEE 5th International Workshop on Evolving Security & Privacy Requirements Engineering (ESPRe)*, pages 1–8. IEEE. DOI: 10.1109/espre.2018.00007.
- Peixoto, M., Gorscheck, T., Mendez, D., Fucci, D., and Silva, C. (2024). A natural language-based method to specify privacy requirements: an evaluation with practitioners. *Requirements Engineering*, pages 1–23. DOI: 10.1007/s00766-024-00428-z.
- Peixoto, M., Silva, C., Araújo, J., Gorscheck, T., Vasconcelos, A., and Vilela, J. (2023). Evaluating a privacy requirements specification method by using a mixed-method approach: results and lessons learned. *Requirements Engineering*, 28(2):229–255. DOI: 10.1007/s00766-022-00388-2.
- Peixoto, M., Silva, C., Lima, R., Araújo, J., Gorscheck, T., and Silva, J. (2019). Pcm tool: Privacy requirements specification in agile software development. In *Anais Estendidos do X Congresso Brasileiro de Software: Teoria e Prática*, pages 108–113. SBC. DOI: 10.5753/cbsoft_e.stendido.2019.7666.
- Peixoto, M. M. and Silva, C. (2018). Specifying privacy requirements with goal-oriented modeling languages. In *Proceedings of the XXXII Brazilian symposium on software engineering*, pages 112–121. DOI: 10.1145/3266237.3266270.
- Peixoto, M. M., Silva, C., Maia, H., and Araújo, J. (2020). Towards a catalog of privacy related concepts. In *REFSQ Workshops*. Available at: <https://ceur-ws.org/Vol-2584/PT-paper5.pdf>.
- Perera, C., Barhamgi, M., Bandara, A. K., Ajmal, M., Price, B., and Nuseibeh, B. (2020). Designing privacy-aware internet of things applications. *Information Sciences*, 512:238–257. DOI: 10.1016/j.ins.2019.09.061.
- Piras, L., Calabrese, F., and Giorgini, P. (2020). Applying acceptance requirements to requirements modeling tools via gamification: a case study on privacy and security. In *The Practice of Enterprise Modeling: 13th IFIP Work-*

- ing Conference, PoEM 2020, Riga, Latvia, November 25–27, 2020, *Proceedings 13*, pages 366–376. Springer. DOI: 10.1007/978-3-030-63479-7_25.
- Pullonen, P., Tom, J., Matulevičius, R., and Toots, A. (2019). Privacy-enhanced bpmn: enabling data privacy analysis in business processes models. *Software and Systems Modeling*, 18:3235–3264. DOI: 10.1007/s10270-019-00718-z.
- Radics, P. J., Gracanin, D., and Kafura, D. (2013). Pre-process before you build: Introducing a framework for privacy requirements engineering. In *2013 International Conference on Social Computing*, pages 564–569. IEEE. DOI: 10.1109/socialcom.2013.85.
- Rafiei, M. and van der Aalst, W. M. (2021). Privacy-preserving continuous event data publishing. In *Business Process Management Forum: BPM Forum 2021, Rome, Italy, September 06–10, 2021, Proceedings 19*, pages 178–194. Springer. DOI: 10.1007/978-3-030-85440-9_11.
- Roberts, J. D., DeFranco, J. F., and Kuhn, D. R. (2023). Data block matrix and hyperledger implementation: extending distributed ledger technology for privacy requirements. *Distributed Ledger Technologies: Research and Practice*, 2(2):1–11. DOI: 10.1145/3585539.
- Rösch, D., Schuster, T., Waidelich, L., and Alpers, S. (2019). Privacy control patterns for compliant application of GDPR. In *25th Americas Conference on Information Systems, AMCIS 2019, Cancún, Mexico, August 15-17, 2019*. Association for Information Systems. Available at: https://aisel.aisnet.org/amcis2019/info_security_privacy/info_security_privacy/27.
- Salnitri, M., Angelopoulos, K., Pavlidis, M., Diamantopoulou, V., Mouratidis, H., and Giorgini, P. (2020). Modelling the interplay of security, privacy and trust in sociotechnical systems: a computer-aided design approach. *Software and Systems Modeling*, 19(2):467–491. DOI: 10.1007/s10270-019-00744-x.
- Sangaroonsilp, P., Choetkiertikul, M., Dam, H. K., and Ghose, A. (2023a). An empirical study of automated privacy requirements classification in issue reports. *Automated Software Engineering*, 30(2):20. DOI: 10.1007/s10515-023-00387-9.
- Sangaroonsilp, P., Dam, H. K., Choetkiertikul, M., Ragkhitwetsagul, C., and Ghose, A. (2023b). A taxonomy for mining and classifying privacy requirements in issue reports. *Information and Software Technology*, 157:107162. DOI: 10.1016/j.infsof.2023.107162.
- Santana, E., Vilela, J., and Peixoto, M. M. (2022). Diretrizes para apresentação de políticas de privacidade voltadas à experiência do usuário. In *WER*. DOI: 10.29327/1298262.25-17.
- Santos, S., Haghighi, S., Ghanavati, S., Breaux, T. D., and Norton, T. B. (2024). Patterns of inquiry in a community forum for legal compliance with privacy law. In *2024 IEEE 32nd International Requirements Engineering Conference Workshops (REW)*, pages 251–259. IEEE. DOI: 10.1109/rew61692.2024.00039.
- Savola, R. M. (2010). Towards a risk-driven methodology for privacy metrics development. In *2010 IEEE Second International Conference on Social Computing*, pages 1086–1092. IEEE. DOI: 10.1109/socialcom.2010.161.
- Schlehahn, E. and Wenning, R. (2018). GDPR transparency requirements and data privacy vocabularies. In Kosta, E., Pierson, J., Slamanig, D., Fischer-Hübner, S., and Krenn, S., editors, *Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data - 13th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School, Vienna, Austria, August 20-24, 2018, Revised Selected Papers*, volume 547 of *IFIP Advances in Information and Communication Technology*, pages 95–113. Springer. DOI: 10.1007/978-3-030-16744-8_7.
- Shah, T. and Patel, P. (2023). Design of a privacy taxonomy in requirement engineering. In *International Conference on IoT Based Control Networks and Intelligent Systems*, pages 703–716. Springer. DOI: 10.1007/978-981-99-6586-1_47.
- Shelby, L. B. and Vaske, J. J. (2008). Understanding meta-analysis: A review of the methodological literature. *Leisure Sciences*, 30(2):96–110. DOI: 10.1080/01490400701881366.
- Sheth, S., Kaiser, G., and Maalej, W. (2014). Us and them: a study of privacy requirements across north america, asia, and europe. In *Proceedings of the 36th International Conference on Software Engineering*, pages 859–870. DOI: 10.1145/2568225.2568244.
- Silva, D. P., de Souza, P. C., and de Jesus Gonçalves, T. A. (2018). Early privacy: Approximating mental models in the definition of privacy requirements in systems design. In *Proceedings of the 17th Brazilian Symposium on Human Factors in Computing Systems*, pages 1–10. DOI: 10.1145/3274192.3274211.
- Silva, K. and Sarkis, L. (2023). Análise de conformidade da lgpd nas instituições públicas de ensino superior no brasil sob a perspectiva dos profissionais de tic. In *WER*. Available at: http://wer.inf.puc-rio.br/WERpapers/artigos/artigos_WER23/WER_2023_paper_21.pdf.
- Sindre, G. and Opdahl, A. L. (2005). Eliciting security requirements with misuse cases. *Requirements engineering*, 10:34–44. DOI: 10.1007/s00766-004-0194-4.
- Spiekermann, S. and Cranor, L. F. (2008). Engineering privacy. *IEEE Transactions on software engineering*, 35(1):67–82. DOI: 10.1109/tse.2008.88.
- Stach, C. and Mitschang, B. (2019). Elicitation of privacy requirements for the internet of things using accessors. In *Information Systems Security and Privacy: 4th International Conference, ICISSP 2018, Funchal-Madeira, Portugal, January 22-24, 2018, Revised Selected Papers 4*, pages 40–65. Springer. DOI: 10.1007/978-3-030-25109-3_3.
- Stach, C. and Steimle, F. (2019). Recommender-based privacy requirements elicitation-epicurean: an approach to simplify privacy settings in iot applications with respect to the gdpr. In *Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing*, pages 1500–1507. DOI: 10.1145/3297280.3297432.
- Stary, C. and Heininger, R. (2022). Privacy by sharing autonomy—a design-integrating engineering approach. In *International Conference on Subject-Oriented Business Process Management*, pages 3–22. Springer. DOI: 10.1007/978-3-031-19704-8_1.

- Sâmmara ellen Renner Ferrão, Geovana Ramos Sousa Silva, E. D. C. F. F. M. (2024). Towards a taxonomy of privacy requirements based on the LGPD and ISO/IEC 29100. *Inf. Softw. Technol.*, 168:107396. DOI: 10.1016/J.INFSOF.2024.107396.
- Terra, A. H., Vilela, J., and Peixoto, M. M. (2022). A catalog of quality criteria to guide the assessment of applications' privacy policies. In *WER*. Available at: http://wer.inf.puc-rio.br/WERpapers/artigos/artigos_WER22/WER_2022_Camera_ready_paper_37.pdf.
- Thapa, C. and Camtepe, S. (2021). Precision health data: Requirements, challenges and existing techniques for data security and privacy. *Computers in biology and medicine*, 129:104130. DOI: 10.1016/j.combiomed.2020.104130.
- Tsohou, A., Magkos, E., Mouratidis, H., Chrysoloras, G., Piras, L., Pavlidis, M., Debussche, J., Rotoloni, M., and Gallego-Nicasio Crespo, B. (2020). Privacy, security, legal and technology acceptance elicited and consolidated requirements for a gdpr compliance platform. *Information & Computer Security*, 28(4):531–553. DOI: 10.1108/ics-01-2020-0002.
- Valença, G., Sarinho, M. W., Polito, V., and Lins, F. (2022). Do platforms care about your child's data? a proposal of legal requirements for children's privacy and protection. In *WER*. DOI: 10.29327/1298262.25-19.
- Veseli, F., Olvera, J. S., Pulls, T., and Rannenberg, K. (2019). Engineering privacy by design: lessons from the design and implementation of an identity wallet platform. In *Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing*, pages 1475–1483. DOI: 10.1145/3297280.3297429.
- Vieira, A., Peixoto, M. M., and Silva, C. (2023). Um modelo de conceitos relacionados à privacidade de dados pessoais. In Antonelli, L., Lucena, M., and Portugal, R. L. Q., editors, *Anais do WER23 - Workshop em Engenharia de Requisitos, Porto Alegre, RS, Brasil, August 15-17, 2023*. LFS (UFRN, Brasil). DOI: 10.29327/1298356.26-6.
- Wohlin, C., Runeson, P., Höst, M., Ohlsson, M. C., Regnell, B., Wesslén, A., Wohlin, C., Runeson, P., Höst, M., Ohlsson, M. C., et al. (2012). Systematic literature reviews. *Experimentation in software engineering*, pages 45–54. DOI: 10.1007/978-3-642-29044-2_4.
- Yu, E., Liu, L., and Mylopoulos, J. (2007). A social ontology for integrating security and software engineering. In *Integrating security and software engineering: Advances and future visions*, pages 70–106. IGI Global. DOI: 10.4018/9781599041476.ch004.
- Zhao, Q., Shu, L., Li, K., Ferrag, M. A., Liu, X., and Li, Y. (2024). Security and privacy in solar insecticidal lamps internet of things: Requirements and challenges. *IEEE/CAA Journal of Automatica Sinica*, 11(1):58–73. DOI: 10.1109/jas.2023.123870.
- Zimmermann, C. (2016). Framework and requirements for reconciling digital services and privacy. In *24th European Conference on Information Systems, ECIS 2016, Istanbul, Turkey, June 12-15, 2016*, page Research Paper 31. Available at: http://aisel.aisnet.org/ecis2016_rp/31.
- Zinsmaier, S. D., Langweg, H., and Waldvogel, M. (2020). A practical approach to stakeholder-driven determination of security requirements based on the gdpr and common criteria. In *ICISSP*, pages 473–480. DOI: 10.5220/0008960604730480.