Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Ciência da Computação

Técnicas, métodos, processos, frameworks e ferramentas para elicitar requisitos de privacidade: Uma revisão de literatura

Stefano Luppi Spósito

Dissertação apresentada como requisito parcial para
conclusão do Mestrado em Informática

Orientadora
Prof.a Dr.a Edna Dias Canedo

Brasília
2025

Ficha catalográfica elaborada automaticamente,
com os dados fornecidos pelo(a) autor(a)

Luppi Spósito, Stefano
LS764t Técnicas, métodos, processos, frameworks e ferramentas para elicitar requisitos de privacidade: Uma revisão de literatura / Stefano Luppi Spósito; orientador Edna Dias Canedo. Brasília, 2025.
109 p.

Dissertação(Mestrado em Informática) Universidade de Brasília, 2025.

1. Privacidade. 2. Requisitos de Privacidade. 3. Engenharia de Requisitos. I. Dias Canedo, Edna, orient. II. Título.

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Ciência da Computação

Técnicas, métodos, processos, frameworks e ferramentas para elicitar requisitos de privacidade: Uma revisão de literatura

Stefano Luppi Spósito

Dissertação apresentada como requisito parcial para
conclusão do Mestrado em Informática

Prof.a Dr.a Edna Dias Canedo (Orientadora)
Universidade de Brasília (UnB)

Prof. Dr. Geraldo Pereira Rocha Filho
Universidade Estadual do Sudoeste da Bahia, UESB

Prof. Dr. Davi Viana dos Santos
Universidade Federal do Maranhão, UFMA

Prof.a Dr.a Cláudia Nalon
Coordenadora do Programa de Pós-graduação em Informática

Brasília, 29 de Julho de 2025

Dedicatória

Dedico este trabalho à Deus, aos amigos e minha família, que me apoiaram em todo momento e me deram forças para continuar.

Agradecimentos

Agradeço primeiramente a Deus, que permitiu e me deu forças para alcançar os objetivos durante toda minha vida. Agradeço imensamente à minha família, pelo apoio e incentivo nos momentos difíceis e que sempre lutou por minha educação e nunca deixou de acreditar. Agradeço aos meus amigos e a todos que me apoiaram, em especial, Marya Heduarda, por estar sempre ao meu lado. Agradeço especialmente à professora Edna Dias Canedo, por todo apoio, suporte e excelente orientação.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES), por meio do Acesso ao Portal de Periódicos.

Resumo

Contexto: A Engenharia de Requisitos (ER) depende da colaboração de várias funções — como engenheiros de requisitos, stakeholders e desenvolvedores — e de várias técnicas, métodos, processos, frameworks e ferramentas. Isso torna a ER um processo altamente dependente de humanos que se beneficia muito do suporte de ferramentas. Entender como essas técnicas, métodos, processos, estruturas e ferramentas são aplicados nas fases da ER pode fornecer um entendimento valiosos sobre maneiras de aprimorar o processo de ER, contribuindo para resultados mais bem-sucedidos. **Objetivo:** O objetivo principal deste estudo é identificar as técnicas, métodos, processos, frameworks e ferramentas aplicadas em diferentes fases da engenharia de requisitos — como elicitação, análise, especificação, validação e gerenciamento — para abordar os requisitos de privacidade. **Método:** Conduziu-se uma revisão sistemática da literatura (RSL) e foram identificados 125 estudos primários, juntamente de um survey com 37 profissionais. **Resultados:** Durante a revisão, identificou-se uma variedade de técnicas, métodos, processos, frameworks e ferramentas para abordar os requisitos de privacidade. A maioria dos estudos foi conduzida em contextos acadêmicos, com as ferramentas mais frequentemente usadas sendo: PriS Method, Secure Tropos, LINDDUN, i* (i-star), STRAP (Structured Analysis for Privacy), Privacy by Design (PbD) e SQUARE. Além disso, mais de 75% dos estudos aplicaram essas ferramentas na fase de elicitação de requisitos de privacidade. Na indústria, a maioria das técnicas identificadas na literatura não são conhecidas ou usadas por profissionais, com base no survey realizado. **Conclusão:** Este estudo fornece uma análise abrangente de técnicas e ferramentas para requisitos de privacidade em ER, revelando um forte foco em contextos acadêmicos com aplicação limitada na indústria. Pesquisas futuras devem explorar a escalabilidade e eficácia dessas ferramentas em ambientes do mundo real, bem como as razões pelas quais os profissionais não as usam.

Palavras-chave: Técnicas, Métodos, Processos, Frameworks, Ferramentas, Requisitos de privacidade

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

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Abreviaturas e Siglas

GDPR Regulamento Geral sobre a Proteção de Dados.

LGPD Lei Geral de Proteção de Dados.

RSL Revisão Sistemática de Literatura.

Capítulo 1

Introdução

Esse capítulo apresenta uma contextualização para o conteúdo deste estudo, juntamente com o problema de pesquisa que motivou a realização deste trabalho. Adicionalmente, o capítulo apresenta a metodologia utilizada para alcançar os resultados esperados e os apresenta, respectivamente. Por fim, o capítulo apresenta a organização do manuscrito como um todo.

1.1 Contextualização

No mundo cada vez mais digital de hoje, a privacidade se tornou uma preocupação importante no desenvolvimento de software [2, 3]. À medida que o volume de dados pessoais processados por aplicativos e sistemas cresce, garantir a privacidade é um requisito legal e uma responsabilidade ética fundamental. O desafio de integrar a privacidade ao desenvolvimento de software está em identificar as técnicas, métodos, processos, estruturas e ferramentas apropriados que podem efetivamente abordar as preocupações com a privacidade durante todo o ciclo de vida do software [4, 5, 6].

Da elicitação e gerenciamento de requisitos até os estágios finais do desenvolvimento e implantação, a privacidade deve ser considerada em todas as etapas para evitar riscos potenciais, violações e não conformidade com regulamentações como o Regulamento Geral sobre a Proteção de Dados (GDPR) [7] e a Lei Geral de Proteção de Dados (LGPD) [8]. Além disso, o interesse em sistemas baseados em Inteligência Artificial (IA) tem crescido acelerado, tanto entre equipes de desenvolvimento de software quanto na sociedade em geral. Como resultado, as preocupações com privacidade também aumentaram na mesma proporção [2, 3].

À medida que as tecnologias de IA são cada vez mais integradas em vários aplicativos, de serviços personalizados a análises preditivas, a quantidade de dados confidenciais sendo processados aumentou, levantando desafios significativos de privacidade e segurança. Isso

intensifica a necessidade de medidas de privacidade robustas e design com consciência de privacidade em sistemas de IA para garantir que os dados do usuário sejam tratados de forma responsável e em conformidade com os regulamentos em evolução [3]. Um dos aspectos críticos para abordar as preocupações com a privacidade no desenvolvimento de software é a aplicação de técnicas eficazes de engenharia de requisitos. Em particular, entender e aplicar as técnicas existentes nas fases da engenharia de requisitos, como elicitação, especificação, validação e gerenciamento, é fundamental para garantir que os requisitos de privacidade sejam adequadamente definidos, priorizados e incorporados ao design do sistema. Essas técnicas fornecem abordagens estruturadas para identificar necessidades de privacidade, avaliar potenciais riscos de privacidade e garantir que a privacidade seja mantida durante todo o processo de desenvolvimento [4].

Outro problema consiste no fato da privacidade ter várias definições na literatura, mas geralmente convergindo para o mesmo princípio fundamental. Westin [9] define privacidade como "a reivindicação de indivíduos, grupos ou instituições de determinar por si mesmos quando, como e em que medida as informações sobre eles são comunicadas a outros". Pfleeger [10] define privacidade como conhecimento sobre uma pessoa em termos de comunicações e atividades e, portanto, o direito de controlar quem conhece certos aspectos sobre uma pessoa, sua comunicação e suas atividades.

Para garantir que o software proteja adequadamente os dados do usuário, é necessário definir os requisitos de privacidade durante as fases da engenharia de requisitos. Esses requisitos de privacidade devem ser baseados nos dados do usuário pretendidos [11], [12] ou mesmo derivados dos aspectos sociais da privacidade por meio da análise comportamental [13]. Os requisitos de privacidade geralmente se alinham com a legislação ou regulamentos de privacidade de dados em um determinado país [4]. Entre as estruturas legais atuais estão o Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia [7] e a Lei Geral de Proteção de Dados (LGPD) do Brasil [14, 15]. Para que um projeto de desenvolvimento de software esteja em conformidade com essas regulamentações, os requisitos de privacidade devem garantir a proteção dos dados do usuário em todos os sistemas desenvolvidos pelas organizações [16].

O processo de engenharia de privacidade no ciclo de vida de desenvolvimento de software (SDLC) começa identificando e definindo os requisitos de privacidade [17]. Esta fase é particularmente desafiadora devido à complexidade das leis de privacidade e à necessidade de equilibrar as preocupações com a privacidade com outros requisitos concorrentes. Para projetar e implementar sistemas de preservação de privacidade de forma eficaz, técnicas, métodos, estruturas e ferramentas robustas são necessárias. A engenharia de privacidade envolve várias abordagens, incluindo o uso de regulamentações para estabelecer requisitos de privacidade e avaliar ativos organizacionais para atender às necessidades de privacidade

[17].

Ao sintetizar os achados da literatura e da indústria, este estudo contribui para promoção do conhecimento e visibilidade sobre diversas metodologias e frameworks, classificadas em diferentes contextos, que auxiliam a definição e implementação dos requisitos de privacidade nas diversas fases da Engenharia de Requisitos. Entende-se que a criação de um catálogo de metologias e frameworks não apenas aumentará a visibilidade de diversas estratégias ainda desconhecidas para engenheiros de requisitos, como também auxiliará na redução da lacuna entre ferramentas utilizadas na literatura com as ferramentas utilizadas na indústria.

1.2 Problema de Pesquisa

Como apresentado anteriormente, a privacidade se tornou uma preocupação importante no desenvolvimento de software. Devido a este fator, o problema de pesquisa abordado nesta dissertação surge da crescente complexidade envolvida na integração dos requisitos de privacidade ao longo das fases da engenharia de requisitos (ER) no desenvolvimento de software [18]. Com a ampliação do uso de sistemas digitais e o aumento exponencial da coleta e tratamento de dados pessoais, assegurar a privacidade tem sido uma grande preocupação no contexto do desenvolvimento de software [2, 3]. Entretanto, incorporar a privacidade de forma eficaz durante todo o processo de desenvolvimento ainda representa um desafio significativo, sobretudo pela dificuldade de traduzir exigências legais em especificações técnicas claras e práticas [19].

Apesar da existência de diversas técnicas, métodos, processos, frameworks e ferramentas voltadas para tratar os requisitos de privacidade [4], há uma lacuna evidente entre a teoria proposta na literatura acadêmica e a prática observada na indústria. Muitos dos recursos desenvolvidos são pouco conhecidos ou utilizados por profissionais do mercado, especialmente fora do ambiente acadêmico.

1.3 Objetivo Geral

Em uma tentativa de auxiliar e solucionar o problema de pesquisa apresentado, o principal objetivo deste trabalho consiste em identificar e classificar as técnicas, métodos, processos, frameworks e ferramentas utilizados nas diferentes fases da Engenharia de Requisitos para apoiar a definição e implementação dos requisitos de privacidade. Além disso, pretende-se avaliar como essas abordagens são aplicadas em contextos acadêmicos e industriais juntamente da identificação dos principais desafios encontrados na prática.

Para atingir o objetivo geral, foram definidos os seguintes objetivos específicos:

- Realizar uma revisão sistemática de literatura para identificar os estudos que tratam da Engenharia de Requisitos (ER) voltada para requisitos de privacidade;
- Identificar as técnicas, métodos, processos, frameworks e ferramentas utilizadas para realizar a elicitação, análise, especificação, validação e gestão dos requisitos de privacidade;
- Identificar se as ferramentas utilizadas na literatura são usadas pelos profissionais da indústria de software;
- Identificar as dificuldades encontradas na utilização de técnicas, métodos, processos, frameworks e ferramentas na Engenharia de Requisitos para lidar com os requisitos de privacidade;
- Desenvolver um catálogo dos frameworks encontrados ao longo da Revisão Sistemática de Literatura, juntamente das principais metodologias utilizadas pelos estudos aceitos.

1.4 Metodologia

Para alcançar os objetivos propostos, este estudo adotou uma abordagem metodológica baseada em uma Revisão Sistemática de Literatura (RSL), complementada por uma pesquisa empírica realizada por meio de um survey com profissionais da indústria de software. A RSL foi conduzida com base nas diretrizes propostas por Kitchenham *et al.* [20], assegurando um processo rigoroso, replicável e isento de vieses. A metodologia foi estruturada em etapas bem definidas, incluindo a formulação de perguntas de pesquisa, definição de critérios de inclusão e exclusão, construção de strings de busca, seleção das bases de dados, aplicação dos critérios de qualidade e extração dos dados relevantes.

Complementando a análise da literatura, foi conduzido um survey com 37 profissionais da indústria com o objetivo de compreender como as abordagens identificadas na literatura são conhecidas, percebidas e aplicadas na prática. Essa combinação de métodos possibilitou uma comparação entre a perspectiva acadêmica e a prática profissional, permitindo não apenas mapear o estado da arte sobre requisitos de privacidade, mas também revelar lacunas, desafios e oportunidades de alinhamento entre teoria e aplicação. A Figura 1.1 apresenta uma visão geral dos passos executados para desenvolver essa pesquisa. O detalhamento completo da metodologia será apresentado no Capítulo 3.

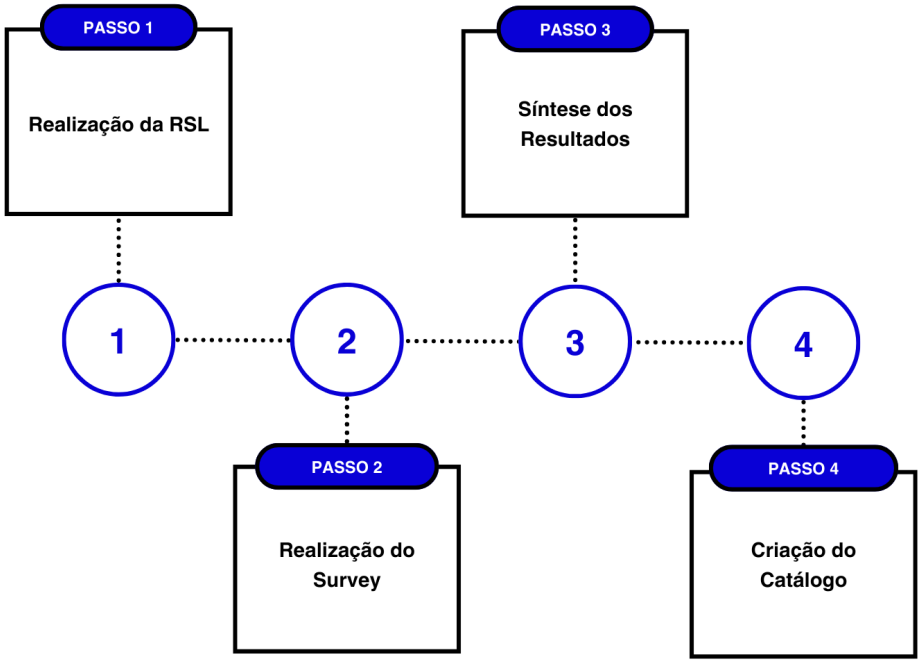


Figura 1.1: Etapas da Metodologia do Estudo

1.5 Resultados Esperados

Como principal contribuição, esta pesquisa resultará na elaboração de um catálogo que reúne, organiza e classifica as abordagens adotadas para o tratamento dos requisitos de privacidade nas diferentes fases da engenharia de requisitos. A partir da síntese de evidências provenientes da literatura e da prática profissional, o catálogo visa apoiar os profissionais da área de requisitos na elicitação, análise, especificação, validação e gestão dos requisitos de privacidade. Ao fornecer orientações baseadas em práticas eficazes, o catálogo contribui para reduzir a lacuna entre teoria e prática, além de apoiar o desenvolvimento de sistemas de software em conformidade com regulamentações de proteção de dados, como a Lei Geral de Proteção de Dados (LGPD).

1.6 Publicações

1. SPÓSITO, Stefano Luppi; MOREIRA, Fernando Rocha; CANEDO, Edna Dias. Designing a Training Journey for Privacy and Information Security Practitioners in the Federal Public Administration. In: SIMPÓSIO BRASILEIRO DE SISTEMAS DE INFORMAÇÃO (SBSI), 21ª edição, 2025, Recife/PE. p. 95-104. DOI: https://doi.org/10.5753/sbsi.2025.246040.

1.7 Disponibilidade dos Dados

Todos os artefatos gerados nesta dissertação estão disponíveis em https://zenodo.org/records/15185984.

1.8 Organização da Dissertação

Está dissertação está estruturada em 3 capítulos além deste. Os capítulos estão organizados da seguinte maneira:

- Capítulo 2 - Embasamento Teórico: Este capítulo apresenta os principais conteúdos e conhecimentos que servem para a compreensão e embasamento deste estudo.
- Capítulo 3 - Metodologia: Este capítulo descreve em detalhes da condução da RSL e seus respectivos resultados, juntamente com a condução do survey realizado e o catálogo desenvolvido através dos resultados obtidos.
- Capítulo 4 - Conclusão: Este capítulo apresenta as conclusões dessa dissertação e os trabalhos futuros.

Capítulo 2

Embasamento Teórico

Este capítulo apresenta os conceitos referentes a privacidade, juntamente de legislações ligadas ao mesmo tema, mais especificamente sobre a Lei Geral de Proteção de Dados (LGPD) [8] e o Regulamento Geral sobre a Proteção de Dados (GDPR) [7]. Adicionalmente, o capítulo apresenta conceitos importantes para o entendimento desse trabalho, como a engenharia de requisitos, juntamente de requisitos de privacidade. Por fim, o capítulo apresenta os trabalhos correlatos com os temas abordados.

2.1 Privacidade de Dados

A privacidade é considerada um conceito multifacetado e dinâmico, indo além do simples controle sobre as informações pessoais dos indivíduos [21]. Privacidade se refere ao direito fundamental de cada indivíduo de gerenciar suas informações e decidir como, quando e com quem esses dados serão compartilhados. A privacidade contemporânea não se limita apenas à proteção contra a vigilância estatal ou corporativa, mas abrange também a capacidade de autodeterminação informacional [22].

Veseli *et al.* [23] propuseram três domínios nos quais os engenheiros de privacidade possuem responsabilidade de exercer e promover a privacidade: 1) User sphere – contempla os dispositivos utilizados pelo usuário, onde entende-se que cada usuário deve possuir total controle sobre seus dispositivos e, consequentemente, às informações contidas nos mesmos; 2) Recipient sphere – se refere ao contexto das organizações, onde o engenheiro de software possui a responsabilidade de minimizar os riscos de vazamento de dados confidenciais, juntamente dos riscos de quebra de privacidade; e 3) Joint sphere – que consiste nas companhias que detêm dados pessoais dos indivíduos, onde, similarmente à recipient sphere, o engenheiro de software deve minimizar os riscos de vazamentos de dados, além de utilizar ferramentas adequadas não apenas para garantir a privacidade dos dados, mas também a segurança.

Ainda em 2005, Kalloniatis *et al.* [24] já alertavam sobre a privacidade individual de todos estar em risco internacionalmente por causa do avanço no uso da Internet e já falava sobre a necessidade de uma metodologia para lidar com os requisitos de privacidade. Uma das recomendações dadas pelos autores era de tentar harmonizar internacionalmente as legislações de privacidade. Porém, um dos contrapontos era que isso seria muito difícil de se conseguir principalmente pelas diferenças culturais, e realmente foi o que aconteceu, hoje em dia existem aspectos parecidos nas legislações de cada país, porém não é possível existir somente uma única legislação para todos.

2.2 Regulamento Geral sobre a Proteção de Dados (GDPR)

O Regulamento Geral sobre a Proteção de Dados (GDPR) [7], consiste em um regulamento da União Europeia, reconhecida como Regulamento (UE) 2016/679. Ela estabelece regras referentes a coleta, processamento, armazenamento e compartilhamento de dados pessoais de indivíduos dentro da UE. Desde sua entrada em vigor em 2018, o GDPR [7] vem ganhando crescente destaque e atenção da sociedade, devido às mudanças significativas que estabelece no tratamento de dados pessoais e na proteção da privacidade [25].

No que se refere ao tratamento de dados pessoais, o GDPR [7] não garante aos titulares de dados a propriedade sobre seus dados, mas possibilita o controle sobre o que poderá acontecer com eles, no quesito de armazenamento, finalidade e compartilhamento [26]. Essa garantia está diretamente relacionada com o funcionamento em plataformas e sistemas tecnológicos, uma vez que estes requerimentos afetam a arquitetura que coleta, guarda e trata dados pessoais [27]. Emma *et al.* [28] informam que o GDPR [7] exige um controle extremamente refinado sobre os dados de uma organização, uma vez que, para manter a conformidade com a legislação, é necessário que os dados considerados como identificadores de um titular sejam devidamente documentados em uma base legal. Não apenas isso, mas há ainda a exigência da exclusão de dados que não sejam mais necessários ou não estejam mais em conformidade.

Schlehahn e Wenning [29] apresentam o GDPR [7] como uma resposta necessária para corrigir o desequilíbrio de poder entre indivíduos e organizações em um cenário onde a coleta e o processamento de dados se tornaram massivos e, em diversos casos, opacos. Os autores informam que um dos principais objetivos da regulamentação consiste em fornecer meios aos titulares dos dados para compreender, controlar e, se necessário, contestar o uso de suas informações pessoais. Adicionalmente, Schlehahn e Wenning informam que a transparência consiste em um dos princípios centrais do GDPR [7], estando incorporada

em diversos artigos do regulamento, como os artigos 5, 12 a 15, 25, 30, 33 e 34, por exemplo, assim como apresentado na Tabela 2.1.

Artigo GDPR	Título
Art. 5	Princípios relativos ao tratamento de dados pessoais
Art. 12	Transparência das informações, das comunicações e das regras para exercício dos direitos dos titulares dos dados
Art. 13	Informações a facultar quando os dados pessoais são recolhidos junto do titular
Art. 14	Informações a facultar quando os dados pessoais não são recolhidos junto do titular
Art. 15	Direito de acesso do titular dos dados
Art. 25	Proteção de dados desde a concepção e por padrão
Art. 30	Registos das atividades de tratamento
Art. 33	Notificação de uma violação de dados pessoais à autoridade de controle
Art. 34	Comunicação de uma violação de dados pessoais ao titular dos dados

Tabela 2.1: Exemplos de Artigos da GDPR

2.3 Lei Geral de Proteção de Dados Pessoais (LGPD)

A Lei Geral de Proteção de Dados (LGPD) [8], instituída pela Lei nº 13.709/2018, consiste em uma legislação brasileira que regula o tratamento de dados pessoais, tanto no meio físico quanto digital, por empresas ou organizações públicas e privadas. A lei, inspirada pelo Regulamento Geral sobre a Proteção de Dados (GDPR) [7], possui como objetivo principal a proteção dos direitos fundamentais de liberdade e privacidade, assegurando a transparência no uso de informações pessoais.

A LGPD [8] e o GDPR [7] compartilham diversos princípios, enfatizando a transparência, a necessidade, a segurança e o propósito específico para o uso de dados. Além disso, essas regulamentações concedem aos indivíduos direitos semelhantes, como acesso, correção, exclusão e portabilidade de seus dados, juntamente com o direito de serem informados sobre o uso e o compartilhamento de suas informações.

Rocha *et al.* [30], em sua descrição sobre a LGPD [8], informa sobre sua criação ter como base o GDPR [7] e apresenta os principais princípios de privacidade contidos na legislação brasileira, apresentados na Tabela 2.2. É importante ressaltar que estes princípios em específico são comuns entre ambas as legislações e, por mais que possam

diferir em nomenclatura e abordagens, seguem o mesmo propósito de manter e garantir a privacidade e proteção de dados.

Princípio	**Descrição**
Finalidade (Purpose Limitation)	Os dados devem ser coletados para propósitos específicos, explícitos e legítimos e não podem ser tratados posteriormente de forma incompatível com esses propósitos.
Adequação (Data Minimization)	O tratamento dos dados deve ser compatível com a finalidade informada ao titular e limitado ao mínimo necessário para atingir esse objetivo.
Necessidade (Storage Limitation & Proportionality)	Apenas os dados estritamente necessários para a finalidade declarada devem ser coletados e mantidos pelo menor tempo possível.
Livre Acesso (Access Rights)	Os titulares dos dados têm o direito de acessar suas informações, entender como elas estão sendo tratadas e solicitar correções ou exclusões.
Qualidade dos Dados (Accuracy)	Os dados pessoais devem ser exatos, atualizados e relevantes para os fins do tratamento, garantindo que informações incorretas ou desatualizadas sejam corrigidas ou apagadas.
Segurança (Integrity & Confidentiality)	Medidas técnicas e organizacionais devem ser implementadas para garantir a proteção dos dados, prevenindo acessos não autorizados, vazamentos, destruição acidental ou ilícita.
Prevenção (Proactive Approach & Risk-Based Approach)	Medidas de segurança e boas práticas devem ser adotadas de forma preventiva, reduzindo riscos antes que eles ocorram.
Responsabilização (Accountability)	O controlador dos dados deve demonstrar conformidade com a legislação, adotando boas práticas e documentando as medidas de proteção implementadas.
Transparência (Transparency)	O tratamento de dados pessoais deve ser realizado de forma clara, acessível e compreensível para os titulares.
Prestação de Contas (Accountability)	O controlador de dados deve ser capaz de demonstrar a adoção de medidas eficazes para garantir a conformidade com a legislação de proteção de dados.

Tabela 2.2: Princípios em Comum entre LGPD e GDPR

Além dos princípios de privacidade delineados e definidos pela LGPD [8], Alves e Moisés [31] propuseram padrões de privacidade em conformidade com a legislação, baseados em percepções obtidas por meio de entrevistas com profissionais da área de tecnologia da

informação. Essa iniciativa foi motivada pela necessidade de criar padrões para identificar princípios e garantir a conformidade com as respectivas regulamentações de privacidade.

Adicionalmente, Ferrão *et al.* [14] propuseram uma taxonomia de requisitos de privacidade para auxiliar equipes de desenvolvimento de software a superar os desafios de conformidade legal, especialmente aqueles relacionados à LGPD e à ISO/IEC 29100. Por meio de uma Revisão Sistemática de Literatura (RSL), os autores identificaram 10 estudos primários como base para seu trabalho. Utilizando o Método de Análise de Requisitos Baseado em Objetivos (GBRAM) e a Teoria Fundamentada (Grounded Theory), eles formularam 129 requisitos de privacidade, categorizados em 10 grupos alinhados aos princípios da LGPD e distribuídos em 5 contextos de aplicação: Software, Pesquisa, Governança, Gestão Pública e Infraestrutura. A taxonomia foi validada por meio de um estudo de caso envolvendo projetos de Open Banking em três grandes bancos brasileiros, demonstrando sua utilidade para orientar equipes de software na especificação eficaz de requisitos de privacidade.

Ainda relacionado com o contexto de conformidade legal, Frej *et al.* [32] desenvolveu uma ferramenta automatizada para facilitar a avaliação e a implementação dos princípios da LGPD, com o objetivo de auxiliar organizações a garantir a conformidade com os requisitos de privacidade exigidos pela legislação. Os testes realizados com a ferramenta demonstraram sua eficiência e acessibilidade, oferecendo uma solução prática para enfrentar os desafios regulatórios impostos pela LGPD.

Por fim, Camêlo e Carina [33] propuseram um catálogo de padrões de privacidade e um guia denominado G-Priv para apoiar a especificação de requisitos de privacidade em conformidade com a LGPD. Foi realizada uma pesquisa com 18 profissionais para avaliar o G-Priv, que foi considerado fácil de entender, especialmente na definição dos papéis e responsabilidades dos stakeholders envolvidos nas quatro etapas do guia. Os participantes da pesquisa também destacaram a usabilidade e a eficiência do guia, considerando-o uma ferramenta valiosa para auxiliar analistas de requisitos na especificação de requisitos de privacidade alinhados à conformidade com a LGPD.

2.4 Engenharia de Requisitos

A Engenharia de Requisitos (ER) consiste em um campo essencial dentro da engenharia de software, responsável por identificar, documentar e manter os objetivos, funções e restrições de sistemas de software, sempre em relação ao mundo real em que esses sistemas estão inseridos, como apresentado por Zave [34]. Esse campo envolve tanto a definição precisa do comportamento do software quanto a consideração de sua evolução ao longo do tempo e entre diferentes sistemas relacionados, sendo caracterizado por sua natureza

ampla, interdisciplinar e muitas vezes caótica, dada a dificuldade de traduzir observações informais em representações formais e rigorosas [34].

Bennaceur *et. al* [35] amplia a definição apresentada anteriormente, destacando que a ER não se limita apenas ao domínio técnico do software, mas abrange sistemas sociotécnicos mais amplos, exigindo que sejam considerados também aspectos físicos, econômicos e sociais. Além disso, reforçam que os stakeholders (usuários, patrocinadores, clientes, etc.) estão no centro do processo de ER, participando da elicitação e validação dos requisitos.

A Tabela 2.3 apresenta as diferentes etapas da Engenharia de Requisitos e as respectivas técnicas que podem ser utilizadas para sua execução.

Cheng e Joanne [1] afirmaram que por mais que a Engenharia de Requisitos seja um processo imprescindível, na prática, é um processo difícil, uma vez que a descrição dos requisitos deve ser focada em descrever precisamente um problema a ser resolvido por um software e, quando não ocorre desta maneira, diversos problemas surgem, gerando um entendimento equivocado sobre requisitos, incluindo ambiguidade sobre como atendê-los.

2.5 Requisitos de Privacidade

Os requisitos de privacidade referem-se às condições, padrões e regulamentações que protegem dados pessoais e salvaguardam os direitos de privacidade dos indivíduos [4]. Esses requisitos frequentemente derivam de estruturas legais, como o GDPR e a LGPD, e têm como objetivo definir como os dados pessoais devem ser coletados, processados, armazenados e compartilhados, garantindo transparência, responsabilidade e o direito à privacidade dos indivíduos [4].

O principal objetivo da engenharia de requisitos de privacidade é definir e compreender claramente os requisitos de privacidade de um sistema, garantindo sua integração harmoniosa ao design e ao desenvolvimento do sistema. Esse processo frequentemente envolve a realização de análises de risco, avaliações de ameaças e avaliações de impacto sobre a privacidade para identificar e mitigar possíveis riscos de privacidade [36].

Após a identificação e definição dos requisitos de privacidade, o foco se desloca para o design de soluções que atendam a esses requisitos, um processo conhecido como engenharia de design de privacidade. Essa etapa pode incluir a implementação de tecnologias ou estratégias específicas, como criptografia ou anonimização, para proteger a privacidade e os dados dos usuários. A adoção de uma abordagem baseada em riscos assegura ainda mais que os designs de privacidade estejam alinhados com os princípios estabelecidos de gerenciamento de riscos [17].

Existem diversas técnicas para especificar requisitos de privacidade [4]. Notario *et al.* [37] abordou essa questão a partir de duas perspectivas: uma abordagem orientada a

Fase da ER	Descrição	Possíveis Técnicas
Elicitação (Elicitation)	Consiste no processo de identificar e obter os requisitos a partir das partes interessadas (stakeholders), documentos existentes, regulamentos e outras fontes.	Entrevistas, Questionários, Workshops, Observação, Análise de Documentos, Protótipos
Análise (Analysis)	Os requisitos são refinados, organizados e priorizados, com objetivo de resolver conflitos entre requisitos, detalhá-los e garantir sua viabilidade técnica.	Classificação de Requisitos, Priorização, Modelagem de Requisitos
Especificação (Specification)	Documentação formal de maneira clara e precisa dos requisitos, para que possam ser compreendidos por desenvolvedores, testadores e clientes.	User Stories, Modelos Gráficos, Documento de Especificação de Requisitos de Software (ERS)
Validação (Validation)	Processo de verificar se os requisitos documentados realmente refletem as necessidades e expectativas dos stakeholders e se estão completos, corretos e viáveis para implementação	Revisões, Prototipagem, Análise de Consistência, Verificação de Rastreabilidade
Gestão de Requisitos (Management)	Consiste na etapa responsável por acompanhar e controlar os requisitos ao longo do ciclo de vida do projeto, uma vez que os requisitos podem mudar devido a novas necessidades de stakeholders, mudanças regulatórias ou restrições técnicas.	Controle de Mudanças, Rastreabilidade de Requisitos, Monitoramento do Impacto de Mudanças

Tabela 2.3: Fases da Engenharia de Requisitos e Possíveis Técnicas de Implementação [1]

objetivos e uma abordagem baseada em riscos. A perspectiva orientada a objetivos foca em derivar princípios de privacidade e estabelecê-los como requisitos do sistema, enquanto a perspectiva orientada a riscos consiste nas especificidades do sistema ao longo de seu desenvolvimento. Os objetivos de privacidade ou proteção de dados frequentemente são derivados de princípios fundamentais de privacidade e de estruturas legais.

Adicionalmente, Hansen *et al.* [38] identificou seis objetivos centrais de proteção de

dados, no contexto de tratamento de dados relevantes de privacidade (identificadores, quasi-identificadores), sendo eles:

- Confidencialidade: Se refere a necessidade de sigilo, se referindo a não divulgação de informações de certas entidades no contexto da tecnologia da informação [38];
- Integridade: Se refere a confiabilidade de uma informação, onde há uma necessidade de autenticidade, não modificação e garantia de que os dados estejam corretos [38];
- Disponibilidade: Representa a necessidade de uma determinada informação ser acessível, compreensível e processada em um curto período de tempo [38];
- Desvinculação: O processamento dos dados deve se dar de forma que os dados relevantes de privacidade não sejam vinculáveis a nenhum outro tipo de informação relevante de privacidade fora do domínio de tratamento de dados [38];
- Transparência: Este objetivo está relacionado com o fato de que toda informação relevante de privacidade, incluindo contextos legais, organizacionais e técnicos, podem ser entendidos e reconstruídos a qualquer momento [38];
- Intervenibilidade: O objetivo se refere a possibilidade de intervenção para qualquer tipo de processamento de dados relevantes de privacidade [38].

Diversas metodologias contribuem para um corpo de conhecimento que abrange métodos, ferramentas, bases de conhecimento sobre privacidade, modelos, documentação e outros elementos projetados para ajudar engenheiros de software a criar sistemas que preservem a privacidade [4]. Caiza *et al.* [39] destacara a necessidade urgente de pesquisas adicionais para identificar métodos que apoiem o desenvolvimento de sistemas focados na privacidade de dados. Os autores ressaltaram a importância de ferramentas automatizadas para uma adoção mais ampla na indústria.

2.6 Trabalhos Relacionados

Ferrão et al. [14] propuseram uma taxonomia de requisitos de privacidade para apoiar equipes de desenvolvimento de software na superação de desafios relacionados à conformidade legal, especialmente aqueles associados à LGPD e à norma ISO/IEC 29100. Utilizando uma Revisão Sistemática de Literatura (RSL), os autores identificaram 10 estudos primários como base para o trabalho. Aplicando o método de Análise de Requisitos Baseada em Objetivos (GBRAM) e a Teoria Fundamentada (Grounded Theory), formularam 129 requisitos de privacidade, categorizados em 10 grupos alinhados aos princípios da LGPD e distribuídos em 5 contextos de aplicação: Software, Pesquisa, Governança,

Gestão Pública e Infraestrutura. A taxonomia foi validada por meio de um estudo de caso envolvendo projetos de Open Banking em três grandes bancos brasileiros, demonstrando sua utilidade em orientar equipes de software na especificação eficaz de requisitos de privacidade.

Frej et al. [32] desenvolveram uma ferramenta automatizada para agilizar a avaliação e a implementação dos princípios da LGPD, com o objetivo de auxiliar as organizações a garantirem a conformidade com os requisitos de privacidade exigidos pela legislação. Os testes realizados com a ferramenta demonstraram sua eficiência e acessibilidade, oferecendo uma solução prática para enfrentar os desafios regulatórios impostos pela LGPD.

Camelo e Alves [33] propuseram um catálogo de padrões de privacidade e um guia chamado G-Priv para apoiar a especificação de requisitos de privacidade em conformidade com a LGPD. Foi realizada uma pesquisa com 18 profissionais para avaliar o G-Priv, que se mostrou de fácil compreensão, especialmente na definição dos papéis e responsabilidades das partes interessadas envolvidas nas quatro etapas do guia. Os participantes da pesquisa também destacaram a usabilidade e a eficiência do guia, considerando-o uma ferramenta valiosa para auxiliar analistas de requisitos na especificação de requisitos de privacidade alinhados à conformidade com a LGPD.

Diversas metodologias contribuem para um corpo de conhecimento que abrange métodos, ferramentas, bases de conhecimento sobre privacidade, modelos, documentação e outros elementos voltados a auxiliar engenheiros de software na criação de sistemas que preservem a privacidade. Caiza et al. [39] enfatizaram a necessidade urgente de mais pesquisas para identificar métodos que apoiem o desenvolvimento de sistemas focados na privacidade dos dados. Destacaram ainda a importância de ferramentas automatizadas para uma adoção mais ampla na indústria. Esta pesquisa aborda essa lacuna ao investigar as técnicas, métodos, processos, frameworks e ferramentas utilizados na Engenharia de Requisitos para a elicitação, análise, especificação, validação e gestão de requisitos de privacidade.

Diferentemente dos trabalhos apresentados nesta seção, esta pesquisa apresenta 125 estudos resultantes de uma Revisão Sistemática de Literatura (RSL), focados na área de engenharia de requisitos, especificamente em requisitos de privacidade. Adicionalmente, este estudo também tem como resultado um catálogo que serve para criar uma maior visibilidade para os frameworks e metodologias encontradas ao longo da RSL, separados em diferentes categorias.

Capítulo 3

Metodologia

Este capítulo apresenta e descreve a Revisão Sistemática de Literatura (RSL) realizada neste trabalho. Inicialmente, são apresentados os conceitos fundamentais de uma RSL, juntamente dos critérios utilizados para criar a string de busca. Em seguida, as questões de pesquisa são apresentadas, aprimorando o direcionamento e o propósito desta revisão. Adicionalmente, as buscas nas respectivas bases de dados foram apresentadas, juntamente dos critérios de seleção e qualidade para os artigos a serem selecionados. Por fim, são apresentados os estudos primários, selecionados ao longo da Revisão Sistemática de Literatura, juntamente das respostas para cada uma das questões de pesquisa e, por fim, são discutidas as lacunas na literatura e ameaças a validade desta revisão.

3.1 Revisão Sistemática de Literatura

Neste trabalho, foi realizada uma Revisão Sistemática de Literatura (RSL), também conhecida como revisão sistemática, segundo o protocolo proposto por Kitchenham *et al.* [20]. Esse processo é descrito como um meio de identificar, avaliar e interpretar todas as pesquisas disponíveis que sejam relevantes à uma questão de pesquisa, tópico, área ou fenômeno de interesse, onde, no caso desta pesquisa, consiste no tópico da Engenharia de Requisitos.

Os objetivos da realização de uma revisão sistemática de literatura nesta pesquisa consistem primariamente em identificar e investigar as técnicas, métodos, processos, frameworks e ferramentas utilizadas na literatura e na indústria e, assim, realizar a elicitação, análise, especificação, validação e gerenciamento dos requisitos de privacidade. É importante ressaltar também que uma revisão sistemática proporciona diversos benefícios em uma pesquisa, uma vez que através dela é possível não apenas condensar e resumir evidências de uma tecnologia ou tratamento, por exemplo, como também resumir evidências empíricas e possíveis limitações [20].

Kitchenham *et al.* [20] divide a revisão sistemática de literatura em três etapas principais: Planejamento, Condução e Relato.

- **Planejamento**: Consiste na identificação da necessidade de se realizar uma revisão sistemática, juntamente da criação de questões de pesquisa e protocolos de revisão.
- **Condução**: Etapa de identificação da pesquisa, onde serão selecionados os estudos primários e será realizada a avaliação de qualidade e, posteriormente, a extração, monitoramento e síntese dos dados encontrados e recolhidos.
- **Publicação dos Resultados**: Consiste em especificar mecanismos de disseminação de resultados, juntamente da formação e análise do relatório principal referente a revisão realizada.

No contexto da Revisão Sistemática de Literatura (RSL) deste estudo, a etapa de planejamento consistiu primariamente na definição das questões de pesquisa e estratégias de busca, juntamente das definições de fontes de pesquisa, critérios de seleção e qualidade. A segunda etapa consistiu na identificação dos estudos primários nas bases de dados e que fossem aceitos pelos critérios de qualidade. Esta etapa também abrangeu a extração de dados, juntamente da realização do survey, feito para levantar dados referentes à indústria. Por fim, a síntese de dados serviu como atividade final para a segunda etapa.

A terceira e última etapa, consistindo na publicação dos resultados, se deu através da descrição, disseminação e avaliação dos resultados obtidos, onde, através do formulário de extração e relatos da Seção 3.2, estas atividades puderam ser concluídas. Adicionalmente, a Figura 3.1 apresenta este processo de forma visual através de uma figura adaptada do trabalho de Kitchenham *et al.* [20].

3.1.1 String de Busca

Para a execução da RSL, foi inicialmente definida uma string de busca conforme o conjunto de critérios PICO [40], que consiste em: **População**: o processo de engenharia de requisitos e suas fases (identificação, especificação, validação, verificação e gerenciamento); **Intervenção**: as ferramentas utilizadas para atingir o resultado; **Comparação**: isto não se aplica, uma vez que o objetivo desta pesquisa não é comparar métodos; e **Resultado**: requisitos de privacidade.

O processo de engenharia de requisitos (população) sofre a intervenção de métodos/-ferramentas/processos (intervenção) para gerar requisitos de privacidade (resultado). Baseado neste processo, foi definida uma string de busca primária, sendo adequada para cada base de dados, uma vez que as bases realizam alterações na mesma para que se encaixe em seus padrões de busca, produzindo as strings apresentadas na Tabela 3.1.

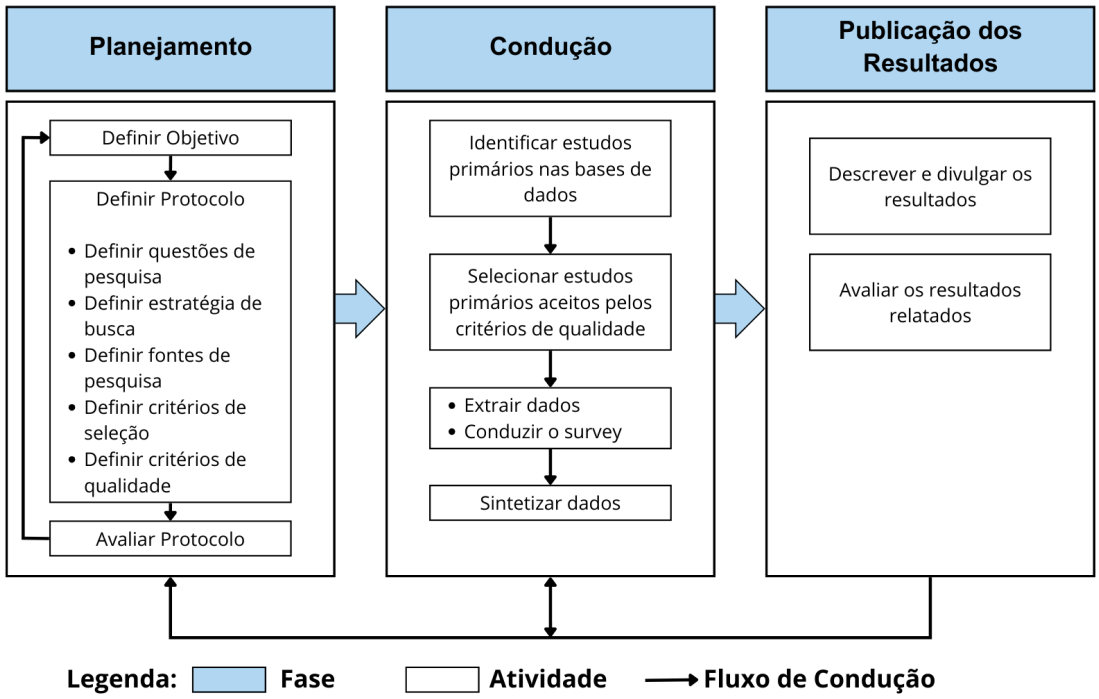


Figura 3.1: Etapas da Revisão Sistemática de Literatura

3.1.2 Questões de Pesquisa

As questões de pesquisa (RQs) foram formuladas com o objetivo de guiar a revisão sistemática e assegurar que o estudo atenda aos objetivos definidos no Capítulo 1. No contexto desta revisão, foram formuladas as questões de pesquisa apresentadas na Tabela 3.2.

Essas questões foram elaboradas com base no critério PICO (Population, Intervention, Comparison, Outcome) [41] para garantir que os aspectos relevantes do domínio de requisitos de privacidade durante a Engenharia de Requisitos sejam investigados de maneira abrangente. As respostas a essas questões permitirão identificar as técnicas, métodos, processos, frameworks e ferramentas, juntamente com os desafios identificados na literatura relacionada a requisitos de privacidade e na indústria, além de suas aplicações em cada etapa da Engenharia de Requisitos.

As questões de pesquisa RQ.1 e RQ.2 possuem como objetivo a identificação das principais ferramentas, técnicas, métodos, processos e frameworks utilizados nas diferentes etapas do processo da engenharia de requisitos. A diferenciação entre "academia" e "indústria" foi considerada relevante, uma vez que diversas ferramentas não possuem sua aplicabilidade comprovada na indústria, entretanto ainda apresentam conceitos, técnicas e informações consideradas valiosas para esta pesquisa. Em relação às ferramentas utilizadas na indústria, decidiu-se realizar um survey com profissionais da área de engenharia de software e engenharia de requisitos para obter respostas da RQ.2.

Base de Dados	String de Busca Utilizada
String Original	"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)

Tabela 3.1: String de Busca por Base de Dados

A questão de pesquisa RQ.3 busca responder como os conhecimentos apresentados nos estudos analisados podem ser aplicados nas respectivas fases da engenharia de requisitos, uma vez que buscou-se exemplos e casos de testes que mostrassem a aplicabilidade das técnicas, métodos, processos, frameworks e ferramentas em contextos preferencialmente reais ou similares, tais como resolução de problemas em aberto na indústria, integração com softwares existentes, surveys com profissionais da área de requisitos, etc.

Por fim, a questão de pesquisa RQ.4 visa os desafios e dificuldades atuais na elicitação

ID	Questão de Pesquisa
RQ.1	Quais as técnicas, métodos, processos, frameworks e ferramentas utilizadas na literatura para realizar o levantamento, análise, especificação, validação e gerenciamento dos requisitos de privacidade em diferentes contextos?
RQ.2	Quais as técnicas, métodos, processos, frameworks e ferramentas utilizadas na indústria para realizar o levantamento, análise, especificação, validação e gerenciamento dos requisitos de privacidade em diferentes contextos?
RQ.3	Como as técnicas, métodos, processos, frameworks e ferramentas identificadas na literatura e na indústria são usadas nas fases da engenharia de requisitos para privacidade?
RQ.4	Quais são os desafios para elicitar os requisitos de privacidade?

Tabela 3.2: Questões de Pesquisa

de requisitos, seja em um contexto específico apresentado pelo artigo ou em um contexto generalizado: "requisitos de privacidade x requisitos de segurança", por exemplo. Além de visar a identificação dos desafios e dificuldades, essa questão abre espaço para o encontro de possíveis soluções para desafios já encontrados anteriormente em pesquisas acadêmicas, uma vez que considerou-se que a descoberta dessas soluções é tão importante quanto a descoberta de novas técnicas, métodos, processos, frameworks e ferramentas.

3.1.3 Busca em Bases de Dados

A string de busca foi utilizada em 4 bases de dados: IEEE Xplore, Web of Science, ACM Digital Library e Scopus. A escolha destas bases de dados foi feita de acordo com as fontes relevantes de Engenharia de Software recomendadas por Kitchenham *et al.* [20]. O acesso às bases de dados foi feito através do Portal de Periódicos da CAPES, utilizando o login da Universidade de Brasília. Após a aplicação da string de busca nas bases digitais, foram retornados 3062 estudos, dispostos entre as quatro bases, conforme apresentado na Figura 3.2.

Após a etapa inicial de extração, todos os bibtex foram baixados e armazenados localmente. Em seguida, os dados duplicados foram tratados utilizando a ferramenta slr-manager, gerando um novo arquivo com todos os bibtex não duplicados. Após a exclusão dos estudos duplicados, foi obtido um total de 1906 estudos, conforme apresentado na Figura 3.2.

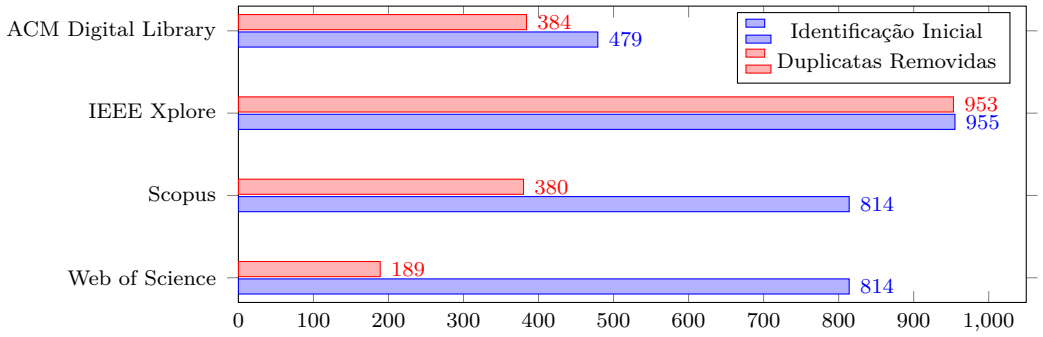


Figura 3.2: Quantidade de Estudos Identificados e Selecionados por Base de Dados Digital

3.1.4 Critérios de Seleção

Para verificar a coerência dos artigos com o propósito da pesquisa, além de sua qualidade e conteúdo, foram definidos critérios de inclusão (IC) e de exclusão (EC) a serem adotados na Revisão Sistemática de literatura.

(IC1) O estudo apresenta técnicas, métodos, processos, frameworks ou ferramentas relacionadas à requisitos de privacidade de software;

(IC2) O estudo é um artigo de pesquisa revisado por pares (ou seja, um artigo de periódico ou documento de conferência);

(EC1) O estudo está fora do contexto de desenvolvimento de software (Ex., estudos sobre VANETS, VICS);

(EC2) O estudo não é um artigo completo (Ex., menos de 6 páginas);

(EC3) O estudo não é um trabalho primário (Ex., revisão de literatura ou trabalho duplicado/ampliado);

(EC4) O estudo não está escrito em um idioma compreendido pelos autores (Ex., que não seja inglês, português ou espanhol).

Tendo como base os critérios de inclusão e exclusão apresentados anteriormente, todos os artigos foram classificados da seguinte maneira:

- Rejected - ABS: O artigo foi rejeitado pelo seu “Abstract”, onde percebeu-se que o conteúdo se encaixava em um dos parâmetros de rejeição ou não estava relacionado com privacidade ou com elicitação de requisitos de privacidade;
- Rejected - FText: O artigo foi rejeitado por não conter o número mínimo de páginas para ser considerado como artigo completo, ou não se trata de um trabalho primário, ou não possui um texto condizente com os parâmetros de aceitação;

- Rejected - QA: O estudo não atende aos critérios de qualidade definidos nesta pesquisa, apresentados na seção 3.1.5;
- Accepted: O artigo atende aos requisitos.

3.1.5 Avaliação de Qualidade

Para assegurar a inclusão de estudos metodologicamente sólidos nesta revisão sistemática, foram definidos critérios específicos de avaliação de qualidade (QA). Esses critérios foram fundamentais para garantir que os estudos selecionados contribuam de forma significativa para a compreensão e avanço das práticas em requisitos de privacidade.

(QA 1) **Clareza na definição do contexto de aplicação:** O estudo descreve claramente o contexto em que as técnicas ou ferramentas de requisitos de privacidade foram aplicadas, como a etapa de engenharia de requisitos, ou o tipo de sistema ou aplicação?

(QA 2) **Rigor metodológico na descrição das técnicas e métodos:** O estudo fornece uma descrição detalhada e metodologicamente rigorosa das técnicas, métodos, processos, frameworks ou ferramentas de requisitos de privacidade utilizadas?

(QA 3) **Evidências empíricas ou teóricas:** O estudo apresenta evidências empíricas (como estudos de caso, experimentos, ou avaliações) ou uma base teórica sólida que suporta o uso das técnicas ou ferramentas propostas para requisitos de privacidade?

(QA 4) **Avaliação da eficácia:** O estudo discute ou avalia a eficácia das técnicas, métodos ou ferramentas na prática? São fornecidos dados ou exemplos que demonstram como as técnicas foram bem-sucedidas ou quais desafios foram encontrados?

(QA 5) **Consideração de aspectos de privacidade específicos:** O estudo aborda aspectos específicos dos requisitos de privacidade, como conformidade com regulamentações (por exemplo, GDPR), proteção de dados sensíveis, ou controle de acesso, de maneira detalhada e relevante?

(QA 6) **Relevância e aplicabilidade prática:** O estudo discute a relevância prática das técnicas ou ferramentas em diferentes contextos de aplicação, e se elas podem ser generalizadas ou adaptadas para outros ambientes ou indústrias?

(QA 7) **Transparência e replicabilidade:** O estudo apresenta os resultados de maneira transparente, com detalhes suficientes para que outros pesquisadores ou profissionais possam replicar as técnicas ou métodos em contextos similares?

É importante ressaltar que todos os critérios foram de igual importância durante a avaliação dos estudos, entretanto, há um destaque especial para os critérios 4 e 7, uma vez que as técnicas, métodos, processos e frameworks precisam possuir uma eficácia comprovada, juntamente da possibilidade de replicação, assim como uma explicação clara caso exista algum desafio em aberto referente ao trabalho apresentado.

3.1.6 Condução da RSL

Ao longo do processo da Revisão Sistemática de Literatura (RSL), 1906 artigos foram analisados, onde 782 estudos foram eliminados por seu abstract e título, 426 foram eliminados pelo seu conteúdo e 93 foram removidos pelos critérios de qualidade de texto, onde não foi possível compreender as técnicas apresentadas ao longo dos respectivos textos. Por fim, 486 artigos foram selecionados para uma avaliação mais detalhada, onde técnicas, métodos, processos, frameworks ou ferramentas relacionadas à engenharia de requisitos foram identificados e catalogados. Ao final, 70 estudos foram classificados como "Accepted", apresentando informações e conteúdos condizentes com os critérios de aceitação e as questões de pesquisa. Adicionalmente, foram encontrados 55 artigos manualmente, através de uma busca feita na base DBLP utilizando a string "Privacy Requirements" e uma busca nos artigos publicados no Workshop em Engenharia de Requisitos (WER), (Requirements Engineering Conference) e (REFSQ), totalizando 125 artigos classificados como aceitos ao fim desta revisão, como apresentado na Tabela A.1.

A Figura 3.3 apresenta de forma visual as etapas do processo de seleção de estudos. "Collecting Papers" representa a etapa de coleta inicial de artigos recuperados das bases digitais, juntamente da quantidade de artigos nas respectivas fases do processo. "Removing Duplicates" representa a etapa de remoção de artigos duplicados e seus resultados; "Removing by Abstract" representa o número de artigos restantes após a aplicação dos critérios de seleção ao título e resumo dos artigos; "Removing by Full-text and QA" se refere a quantidade restante de artigos após aplicação dos critérios de seleção ao texto completo do estudo; "Removing by RE context" consiste na etapa de remoção dos artigos que tratavam de privacidade, porém não tinham nenhuma ligação com o processo de engenharia de requisitos. Por fim, "Selected Papers" apresenta os estudos selecionados para a extração dos dados, enquanto "Manual Research" indica a quantidade de artigos selecionados na busca manual.

3.1.7 Extração de Dados

A etapa de Extração de Dados consiste na coleta e organização de informações relevantes dos estudos selecionados para responder às questões de pesquisa, sendo crucial em um

QA = Quality Assessment ER = Engenharia de Requisitos

Figura 3.3: Etapas do processo de seleção dos estudos

processo de revisão de literatura.

Neste contexto, a extração de dados visa identificar e sintetizar as técnicas, métodos, processos, frameworks e ferramentas utilizados na literatura e na indústria para o levantamento, análise, especificação, validação e gestão dos requisitos de privacidade. Esta etapa foi essencial para garantir a integridade e a replicabilidade da revisão, minimizando vieses e assegurando que todas as evidências sejam consideradas de forma consistente. Além disso, através desta etapa, foi possível realizar uma análise aprofundada dos desafios e lacunas existentes, bem como das práticas mais eficazes na área, contribuindo para a resposta de todas as questões de pesquisa apresentadas anteriormente, juntamente de justificativas e explicações.

Durante a extração, foi possível observar um padrão de publicações ao longo dos anos, assim como ilustrado na Figura 3.4. Com base nesses dados, foi possível concluir que houve uma baixa produção inicial nos anos de 2005 à 2017, tendo em vista a baixa quantidade de artigos aceitos, indicando uma possível limitação de pesquisa ou baixo interesse no tema de Requisitos de Privacidade durante este período.

A partir do ano de 2018 é possível visualizar um crescimento gradual de pesquisas nessa área. Entende-se que este período reflete uma fase de muito interesse e produção na área, indicando um avanço significativo. Supõe-se que este avanço se deve ao fato de leis como Regulamento Geral sobre a Proteção de Dados (GDPR) [7] e Lei Geral de Proteção de Dados (LGPD) [8] terem sido aprovadas e entrarem em vigor durante este período.

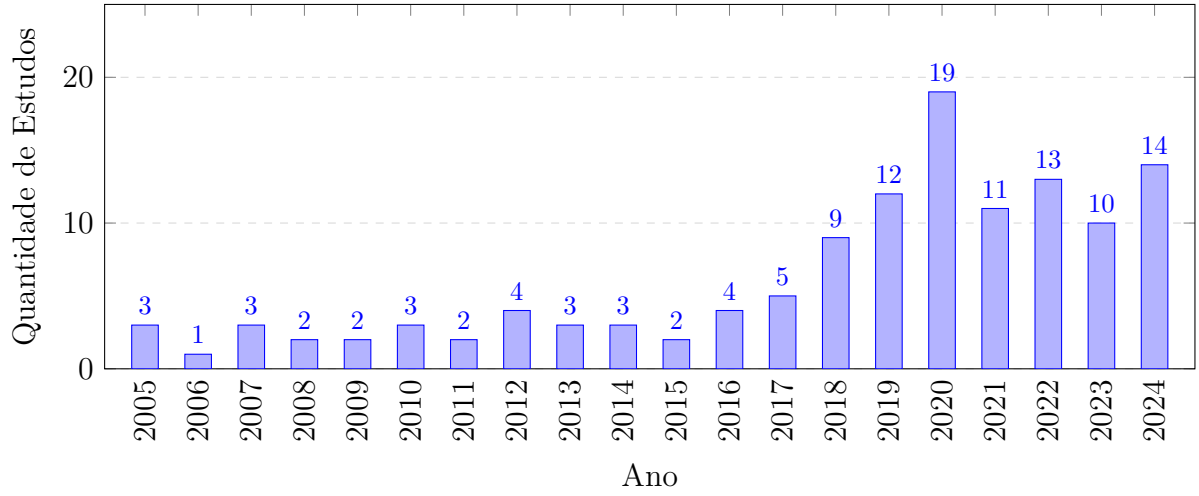


Figura 3.4: Distribuição dos Estudos por Ano de Publicação

Campos de Extração

Os campos de extração de dados foram definidos com o objetivo de responder às questões de pesquisa da Revisão Sistemática de Literatura (RSL) estabelecidas e cobrir todos os aspectos relevantes da literatura e da indústria relacionados aos requisitos de privacidade. Os campos foram organizados em um formulário de extração, onde cada artigo selecionado teve suas principais informações extraídas e armazenadas em cada seção, para fácil acesso. Os campos de extração, apresentados na Tabela 3.3, foram gerados com base no formulário proposto por Hidellaarachchi *et al.* [42] e adaptados para o contexto desta pesquisa. Adicionalmente, optou-se por deixar o formulário de extração, juntamente de seus campos, em inglês, para facilitar a replicabilidade desta pesquisa.

Tabela 3.3: Formulário de Extração de Dados

ID	Extraction Field
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?

3.2 Resultados

Com base nos critérios de seleção apresentados anteriormente, os dados dos 125 estudos aceitos foram extraídos de maneira clara e objetiva no formulário de extração. A partir desses resultados e extrações, foi possível observar o relacionamento de todos os estudos com as respectivas questões de pesquisa, além de identificar as principais técnicas, métodos, processos, frameworks e ferramentas utilizadas no processo de elicitação de requisitos de privacidade e, consequentemente, no processo da engenharia de requisitos. É importante lembrar que houve estudos que não possuíram dados claros o suficiente para preencher todos os campos do formulário de extração, entretanto, esse fator não foi considerado um impedimento, uma vez que os critérios de aceitação e de qualidade já haviam sido aplicados sobre os respectivos estudos e os mesmos foram classificados como aceitos.

A Figura 3.5 apresenta a quantidade de estudos de acordo com o método usado pelo estudo selecionado. Estudos de Caso foram utilizados na maior quantidade de estudos, totalizando 29 estudos primários que utilizam o uso de dessa abordagem para requisitos de privacidade. O segundo método mais utilizado foi a análise de documentação, com 22 estudos. Foi observado o uso de frameworks em 20 estudos, assim como o método de modelagem. Quinze (15) estudos utilizaram o método de survey, 8 utilizaram entrevistas como metodologia principal e, por fim, 10 estudos utilizaram outros métodos (não mencionados quais).

Adicionalmente, outros dados importantes extraídos dos estudos primários foram: Quarenta (40) estudos tiveram seu foco em uma das fases da engenharia de requisitos, apresentando ferramentas específicas para as respectivas fases ou informando como se-

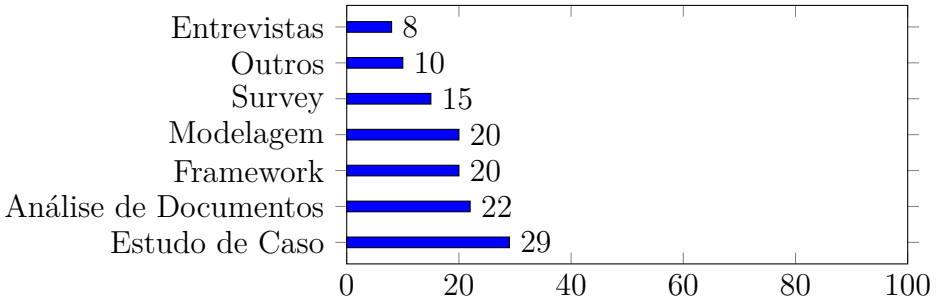


Figura 3.5: Quantidade de Estudos por Métodos

riam afetadas através de seus resultados, são eles: [PS1], [PS2], [PS3], [PS4], [PS5], [PS6], [PS7], [PS8], [PS9], [PS10], [PS11], [PS12], [PS13], [PS14], [PS15], [PS16], [PS17], [PS18], [PS19], [PS20], [PS21], [PS22], [PS23], [PS24], [PS25], [PS26], [PS27], [PS28], [PS29], [PS30], [PS31], [PS32], [PS33], [PS34], [PS35], [PS36], [PS37], [PS38], [PS39], [PS40].

Conforme apresentado na Tabela 3.4, 88 estudos foram desenvolvidos no contexto da academia, ou seja, os autores identificaram ou propuseram técnicas, métodos, processos, frameworks ou ferramentas e realizaram os testes das propostas com estudantes ou em projetos fictícios. Adicionalmente, 33 estudos foram realizados no contexto da indústria, ou seja, os autores realizaram testes das suas propostas usando projetos reais. Em 4 estudos, os autores apenas realizaram um levantamento bibliográfico das técnicas utilizadas e demonstraram uma ilustração da sua aplicação.

Trinta e quatro (34) estudos realizaram uma identificação do relacionamento entre diferentes requisitos de privacidade, como, por exemplo: [PS72] afirma que requisitos de privacidade devem interagir com necessidades de segurança, legais e de aceitação, abordando requisitos como privacy by design, gestão de consentimento e avaliações de impacto de privacidade, ao mesmo tempo que garante a conformidade com as obrigações legais apresentadas na GDPR. Adicionalmente [PS33] identificou a privacidade como um dos seis principais requisitos de segurança no contexto de um sistema IoT, informando que requisitos de privacidade estão ligados a contextos como autenticação, confidencialidade e controle de acesso.

Quinze (15) estudos elencaram os impactos positivos dos requisitos de privacidade na engenharia de requisitos, 6 elencaram impactos negativos e 56 estudos elencaram os impactos positivos e negativos, respectivamente.

De modo geral, os estudos informam que os impactos positivos dos requisitos de privacidade sobre a engenharia de requisitos consistem na melhoria da compreensão e atendimento das necessidades dos stakeholders, apoio à tomada de decisões organizacionais [PS4], orientação para o desenvolvimento de software, e gestão de conformidade regulatória. Ao integrar privacidade desde as fases iniciais, previnem-se violações de direitos,

Contexto	ID do Estudo
Academia	[PS41], [PS42], [PS43], [PS44], [PS45], [PS46], [PS2], [PS47], [PS48], [PS3], [PS49], [PS50], [PS51], [PS52], [PS53], [PS54], [PS55], [PS6], [PS56], [PS57], [PS7], [PS58], [PS59], [PS60], [PS9], [PS61], [PS62], [PS63], [PS64], [PS65], [PS66], [PS10], [PS67], [PS68], [PS69], [PS13], [PS14], [PS70], [PS71], [PS72], [PS73], [PS15], [PS17], [PS74], [PS18], [PS75], [PS76], [PS77], [PS19], [PS78], [PS20], [PS21], [PS23], [PS79], [PS80], [PS81], [PS27], [PS82], [PS28], [PS83], [PS84], [PS29], [PS30], [PS85], [PS86], [PS87], [PS88], [PS32], [PS89], [PS90], [PS33], [PS36], [PS91], [PS37], [PS92], [PS93], [PS94], [PS38], [PS95], [PS96], [PS39], [PS97], [PS98], [PS99], [PS100], [PS101], [PS40]
Indústria	[PS102], [PS103], [PS1], [PS104], [PS105], [PS4], [PS5], [PS106], [PS8], [PS107], [PS108], [PS109], [PS11], [PS12], [PS110], [PS111], [PS112], [PS16], [PS113], [PS114], [PS115], [PS22], [PS116], [PS24], [PS25], [PS26], [PS117], [PS31], [PS34], [PS118], [PS35], [PS119], [PS120], [PS121]
Ilustração	[PS122], [PS123], [PS124], [PS125]

Tabela 3.4: Contextos dos Estudos selecionados

aumenta-se a confiança dos usuários e a transparência no tratamento de dados, além de garantir a conformidade com normas como GDPR e LGPD [PS55], resultando em sistemas mais seguros e projetados com foco na proteção da privacidade.

No contexto de pontos negativos, são mencionados desafios relacionados à complexidade e à confusão gerada pela implementação de regulamentações como o GDPR, incluindo falta de clareza na terminologia e dificuldades para traduzir princípios de privacidade em requisitos de engenharia [PS49]. Outro ponto crítico consiste no conflito entre requisitos de privacidade e outras demandas, como a identidade, particularmente em ambientes de IoT [PS24]. Além disso, a imutabilidade de tecnologias como blockchain pode dificultar a conformidade com regulamentos que exigem a exclusão de dados pessoais. Os estudos também apontam que a inadequada gestão dos requisitos de privacidade pode resultar em software de baixa qualidade e aumentar o risco de sanções legais [PS34].

3.2.1 RQ.1. Quais as técnicas, métodos, processos, frameworks e ferramentas utilizadas na literatura para realizar o levantamento, análise, especificação, validação e gerenciamento dos requisitos de privacidade em diferentes contextos?

Ao longo da análise dos estudos e extração dos respectivos dados, foi observado uma grande quantidade de métodos, processos, frameworks e ferramentas propostas ou utilizadas na literatura nas etapas da Engenharia de Requisitos. Entretanto, foi observado que a grande maioria dos estudos utilizava como embasamento, uma ou mais técnicas, métodos, processos, frameworks e ferramentas já existentes, a Tabela 3.5 apresenta a relação dos estudos com os principais conceitos identificados na literatura:

Nome	Tipo	ID dos Estudos
SQUARE	Processo	[PS104], [PS5], [PS9], [PS66], [PS109], [PS11], [PS75], [PS79]
Secure Tropos	Método	[PS103], [PS45], [PS47], [PS49], [PS51], [PS52], [PS9], [PS61], [PS62], [PS15], [PS74], [PS75], [PS113], [PS20], [PS115], [PS116], [PS79], [PS24], [PS36]
PriS	Método	[PS103], [PS45], [PS2], [PS47], [PS3], [PS49], [PS50], [PS52], [PS6], [PS9], [PS61], [PS108], [PS66], [PS11], [PS110], [PS124], [PS73], [PS15], [PS75], [PS19], [PS114], [PS79], [PS81]
i* (i-star)	Framework	[PS43], [PS103], [PS47], [PS49], [PS52], [PS11], [PS15], [PS113], [PS20], [PS79]
LINDDUN	Método	[PS43], [PS44], [PS49], [PS50], [PS107], [PS9], [PS75], [PS114], [PS79], [PS38], [PS96]
STRAP (STRuctured Analysis for Privacy)	Framework	[PS2], [PS47], [PS49], [PS52], [PS54], [PS15], [PS77], [PS79]
Privacy By Design (PbD)	Método	[PS44], [PS52], [PS55], [PS6], [PS56], [PS107], [PS60], [PS65], [PS13], [PS79], [PS94]

Tabela 3.5: Principais Técnicas, Métodos, Processos, Frameworks e Ferramentas Utilizados nos Estudos Selecionados

SQUARE

O processo de Engenharia de Requisitos de Qualidade e Segurança (SQUARE), criado pelo programa CERT, consiste em um processo que apresenta meios para elicitar, categorizar e priorizar requisitos de segurança durante os estágios iniciais do desenvolvimento de software, consistindo em nove etapas, conforme apresentado em [PS104]:

1. Concordar com as definições.
2. Identificar ativos e objetivos de segurança.
3. Desenvolver artefatos.
4. Executar avaliação de risco.
5. Selecionar técnicas de elicitação.
6. Elicitar requisitos de segurança.
7. Categorizar requisitos.
8. Priorizar requisitos.
9. Inspecionar requisitos.

Por mais que o processo tenha sido originalmente desenvolvido para requisitos de segurança, existem estudos que utilizam e adaptam o método SQUARE para inserir e comportar requisitos de privacidade, assim como [PS5] e [PS66].

O estudo [PS104] apresenta uma adaptação do processo SQUARE para a engenharia de requisitos de privacidade. O estudo aborda o fato de como o processo SQUARE, que possui sua utilização primária no contexto de requisitos de segurança, também pode ser adaptado para ser utilizado no contexto de requisitos de privacidade. Em resumo, o estudo apresenta discussões e modificações necessárias para cada etapa do processo SQUARE, adaptando conforme as necessidades dos requisitos de privacidade.

Secure Tropos

O método Secure Tropos apresentado no estudo [PS74], consistindo em uma extensão da metodologia original Tropos [43], é voltado para a integração de preocupações de segurança no desenvolvimento de sistemas orientados a agentes. O método originalmente desenvolvido para modelagem de requisitos de sistemas multiagentes foi expandido para lidar com requisitos de segurança desde fases inicias da engenharia de requisitos até o seu final.

Analogamente ao processo SQUARE apresentado anteriormente, o método Secure Tropos possui requisitos de segurança como escopo principal, entretanto, ao longo desta revisão sistemática de literatura, foi possível observar que este método permite a adaptação para abranger requisitos de privacidade, como apresentado também em [PS74]. O estudo [PS62] apresenta uma avaliação desta metodologia para requisitos de segurança e privacidade em conjunto. O estudo apresenta sugestões de modificações para o método para uma melhor aplicabilidade em diferentes contextos.

Como prova da possibilidade de integração da metodologia Secure Tropos em requisitos de privacidade, o framework desenvolvido pelo estudo [PS115] é baseado nesta metodologia, permitindo a elicitação de requisitos de privacidade e segurança de legislações e regulamentos relevantes.

Método PriS

O método PriS [PS2] consiste em um método de engenharia de requisitos de segurança, integrando requisitos de privacidade desde o início do processo de desenvolvimento de softwares. O método trata requisitos de privacidade como metas organizacionais e propõe o uso de padrões de processos de privacidade para descrever o impacto dos requisitos de privacidade nos processos de negócio e identificar a arquitetura de sistema que melhor suporta os processos de privacidade. PriS segue quatro atividades principais, sendo elas:

- Elicitação de metas de privacidade.
- Análise de impacto.
- Modelagem de processos afetados.
- Identificação de técnicas de implementação.

Complementando o desenvolvimento do método, o estudo [PS3] propõe uma extensão do PriS, que fornece ferramentas metodológicas que auxiliam os desenvolvedores a estimar as soluções mais adequadas para a implementação de medidas de privacidade no processo de design de software.

i* (i-star) framework

O framework i* (i-star) [44] consiste em uma abordagem orientada a metas e a atores. Sua principal função consiste na captura e análise de interações estratégicas entre agentes ou entidades responsáveis por realizar ações em um sistema, juntamente das motivações que guiam as respectivas interações. O framework pode ser utilizado em diferentes etapas do desenvolvimento de software, tais como na elicitação e análise de requisitos, design de sistemas e análises de organizações.

Alguns dos estudos encontrados utilizam, dentre outros, este framework para embasar e comparar seus respectivos frameworks e modelos desenvolvidos, como apresentado no estudo [PS113]. Onde o framework desenvolvido, em seu processo de avaliação, foi comparado com três outros frameworks, um deles sendo o i*.

LINDDUN

A metodologia LINDDUN, apresentada em [PS43], consiste em uma estrutura sistemática para analisar e abordar questões de privacidade em sistemas, se concentrando principalmente na privacidade desde as etapas iniciais do desenvolvimento de sistemas, facilitando assim a identificação de possíveis ameaças à privacidade.

LINDDUN se baseia na decomposição de ameaças à privacidade em sete categorias principais, representadas pelo acrônimo que gerou seu próprio nome:

- **L**inkability (Vinculação): Preocupa-se com a capacidade de vincular duas ou mais atividades, ou atributos a um único indivíduo.
- **I**dentifiability (Identificabilidade): Refere-se à capacidade de identificar um indivíduo dentro de um conjunto de dados.
- **N**on-repudiation (Não-repúdio): Refere-se à garantia de que um indivíduo não pode negar a autoria de uma ação.
- **D**etectability (Detectabilidade): Trata da capacidade de um atacante detectar se um dado específico está presente ou não em um conjunto de dados.
- **D**isclosure of information (Divulgação de informações): Refere-se ao vazamento de informações pessoais, mesmo quando as informações não estão diretamente associadas a um indivíduo.
- **U**nawareness (Desconhecimento): Envolve a falta de consciência de um indivíduo sobre como seus dados estão sendo usados.
- **N**on-compliance (Não conformidade): Relaciona-se com a falha em aderir às leis e regulamentos de privacidade.

É importante ressaltar que essa metodologia também proporciona uma taxonomia detalhada de ameaças à privacidade e seus impactos, além da sugestão de técnicas específicas de mitigação, dependendo do cenário de desenvolvimento do sistema de dos riscos identificados.

Foi observado que alguns estudos utilizam em seu embasamento e também como referência a metodologia LINDDUN, como apresentado no estudo [PS107], por exemplo,

onde são identificadas 56 ameaças a privacidade que foram categorizadas dentro dessa metodologia, juntamente de recomendações de mecanismos de mitigação adequados para cada uma das ameaças identificadas.

STRAP (STRuctured Analysis for Privacy)

O estudo [PS77] apresenta o framework STRAP, consistindo em uma abordagem leve e estruturada para análise de vulnerabilidades de privacidade no design de sistemas. Este framework utiliza uma análise orientada a metas para identificar vulnerabilidades de privacidade, enquanto as categoriza e propõe soluções ou estratégias de mitigação.

O framework STRAP funciona em quatro etapas, sendo elas:

1. Análise: Os atores, metas e componentes do sistema são identificados e um conjunto de perguntas analíticas é feito para cada meta e submeta.
2. Refinamento: Após a identificação das vulnerabilidades, o próximo passo consiste na tomada de decisão em como eliminá-las ou mitigá-las, dependendo do contexto.
3. Avaliação: Diferentes designs ou soluções são comparados com base na redução de riscos de privacidade.
4. Iteração: O framework suporta um processo iterativo, permitindo a reavaliação do sistema para que possa haver adaptações conforme mudanças ou novas funcionalidades venham a existir.

Como forma de verificação de funcionalidades, o estudo [PS47] realiza uma análise de diversas metodologias relacionadas a requisitos de privacidade, dentre elas o STRAP. Entre seus resultados, o estudo verificou a aplicação deste framework em diferentes fases da engenharia de requisitos e reportou que o framework atende as etapas de Elicitação e Especificação de requisitos. Adicionalmente, o estudo também informa que o framework consegue abordar de forma geral, requisitos negociais de privacidade e segurança.

Privacy by Design (PbD)

Privacy by Design (PbD) [45] consiste em uma abordagem que propõe integrar a privacidade como um princípio fundamental no design e desenvolvimento de sistemas, processos e produtos. O conceito visa garantir que a privacidade seja considerada desde o início e ao longo de todo o ciclo de vida de um projeto, ao invés de tratá-la como uma preocupação secundária ou uma adição posterior.

Os 7 princípios fundamentais do privacy by design são [45]:

1. Proativo, não reativo; preventivo, não corretivo.

2. Privacidade como configuração padrão (Privacy as the Default Setting).
3. Privacidade embutida no design (Privacy Embedded into Design)
4. Funcionalidade total — Ganhos e não uma soma zero (Full functionality: positive-sum, not zero-sum)
5. Segurança durante todo o ciclo de vida da informação (End-to-end security: full lifecycle protection)
6. Transparência e visibilidade (Visibility and transparency: keep it open)
7. Respeito pela privacidade do usuário (Respect for user privacy: keep it user-centric)

Neste contexto, o estudo [PS79] realiza uma análise sobre metodologias de privacidade existentes, onde é verificado se metodologias como LINDDUN, SQUARE e PriS se encaixam no contexto de PbD. O estudo verifica não apenas a conformidade dos frameworks apresentados, mas também seu suporte ao Privacy By Design, apresentando resultados satisfatórios para as metodologias avaliadas, comprovando sua conformidade e suporte ao PbD.

Outras Técnicas

Além das principais Técnicas, Métodos, Processos, Frameworks, Ferramentas apresentadas anteriormente, que possuíram uma maior utilização entre os estudos selecionados, outros poucos estudos utilizaram uma ou mais estratégias que foram consideradas importantes para se fazer menção:

- KAOS method: [PS47], [PS49], [PS52], [PS9], [PS15], [PS75], [PS20]
  - KAOS (Knowledge Acquisition in autOmated Specification) consiste em uma metodologia orientada a metas (goal-oriented) para a engenharia de requisitos, voltada à especificação formal de requisitos e ao desenvolvimento de sistemas complexos [46].
- GBRAM (Goal-Based Requirements Analysis Method): [PS1], [PS47], [PS49], [PS52], [PS15], [PS22]
  - GBRAM (Goal-Based Requirements Analysis Method) consiste em uma metodologia voltada à elicitação e análise de requisitos baseada em metas (goals), com foco em identificar, refinar e organizar requisitos funcionais e não funcionais de um sistema a partir das intenções dos stakeholders [47].
- RBAC (Role-Based Access Control): [PS47], [PS49], [PS52], [PS123], [PS79]

  - RBAC (Role-Based Access Control), se trata de um modelo de controle de acesso amplamente utilizado em sistemas de informação, no qual as permissões de acesso são atribuídas com base nos papéis (roles) que os usuários desempenham dentro de uma organização [48].

- STRIDE: [PS43], [PS107]
  - O modelo STRIDE, desenvolvido pela Microsoft, consiste em uma metodologia para identificação de ameaças de segurança em sistemas de software. Este modelo é utilizado no contexto de modelagem de ameaças (threat modeling), auxiliando equipes de desenvolvimento e segurança a pensarem de forma estruturada sobre os riscos que um sistema pode enfrentar [49].

- PRIPARE: [PS107], [PS10]
  - PRIPARE consiste em uma metodologia de engenharia de privacidade estruturada, desenvolvida para integrar as melhores práticas de privacidade ao longo de todo o ciclo de vida de desenvolvimento de sistemas, com o objetivo de operacionalizar o conceito de Privacy by Design e resolver lacunas existentes entre regulamentações legais e práticas técnicas [50].

- P-STORE: [PS10], [PS67]
  - P-STORE se caracteriza como uma metodologia de engenharia de requisitos de privacidade, criada a partir da metodologia STORE (Security Threat Oriented Requirements Engineering), cujo objetivo principal é guiar de forma sistemática a elicitação de requisitos de privacidade durante o desenvolvimento de sistemas, de forma mais específica em contextos onde dados pessoais são tratados [PS67].

- ISO 29100: [PS55], [PS60], [PS78], [PS22]
  - A ISO/IEC 29100, publicada pela Organização Internacional de Normalização (ISO) e pela Comissão Eletrotécnica Internacional (IEC), consiste em uma norma internacional que estabelece um framework de privacidade para ajudar organizações a proteger informações pessoalmente identificáveis (PII – Personally Identifiable Information) [51].

- Bellotti-Sellen Framework: [PS47], [PS15], [PS77]
  - O Framework Bellotti-Sellen consiste em um framework de design para privacidade em ambientes de computação ubíqua, com foco na preservação da privacidade dos usuários em sistemas que capturam, processam e distribuem dados pessoais continuamente — como os chamados “media spaces”[52].

- M-N (Moffett-Nuseibeh Framework): [PS47], [PS52], [PS15]
  - O Framework M-N (Moffett-Nuseibeh) se trata de uma abordagem sistemática para a engenharia de requisitos de segurança, cujo objetivo é conectar objetivos de segurança aos requisitos funcionais e ao contexto do sistema [53].
- SecTro: [PS51], [PS62], [PS11], [PS32]
  - A ferramenta SecTro consiste em uma aplicação construída através da linguagem de programação Java, que tem como principal funcionalidade o suporte ao desenvolvedor na modelagem das atividades do método Secure Tropos [54].
- PCM (Privacy Criteria Method): [PS9], [PS12], [PS110], [PS31]
  - PCM (Privacy Criteria Method) se trata de um método para guiar desenvolvedores de software na especificação de requisitos de privacidade, podendo ser utilizado com qualquer técnica de especificação de requisitos [55].
- ConfIS: [PS51], [PS32]
  - ConfIS se caracteriza como um framework que tem como objetivo a identificação de conflitos entre requisitos de privacidade e segurança, permitindo que estes conflitos sejam analisados e tratados pelo programador do sistema [56].
- SepTA: [PS11], [PS32]
  - SePTA (Security, Privacy and Trust Approach) se trata de um método que suporta a especificação unificada de requisitos de segurança, privacidade e confiança, através de um framework que auxilia engenheiros de software a reforçar estes requisitos [57].
- Privacy Impact Assessment (PIA): [PS44], [PS10], [PS112], [PS82], [PS40]
  - Privacy Impact Assessment (PIA) pode ser definido como uma metodologia para avaliar os impactos na privacidade de um projeto ou política, servindo como ponto inicial para tomar ações que minimizem ou evitem impactos negativos neste contexto [58].
- Asia-Pacific Economic Cooperation (APEC) Privacy Framework: [PS1], [PS48], [PS82]
  - O APEC Privacy Framework consiste em um framework criado pela Asia-Pacific Economic Cooperation (APEC) com o objetivo de promover a proteção

da privacidade de dados pessoais no contexto do comércio eletrônico entre os países membros da região Ásia-Pacífico [59].

- Non-Functional Requirement Framework (NFR): [PS47], [PS49], [PS52], [PS59], [PS9], [PS113], [PS30], [PS90]
  - O Non-Functional Requirement Framework (NFR) se trata de uma abordagem estruturada para identificar, organizar e tratar de requisitos não funcionais em projetos de software [60].
- OECD Privacy Statement Generator: [PS5], [PS66]
  - O OECD Privacy Statement Generator tem como objetivo apresentar recomendações para governos e organizações sobre como elaborar avisos de privacidade simplificados, baseando-se em iniciativas práticas e pesquisas realizadas por entidades públicas e privadas [61].
- NIST: [PS106], [PS82], [PS29]
  - O Framework de Cibersegurança do NIST apresenta um guia para gerenciamento de riscos de cibersegurança, servindo para auxiliar organizações a diminuírem os riscos neste contexto [62].

Adicionalmente, o estudo [PS20] apresenta um catálogo de conceitos relacionados a privacidade, sendo eles: 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, Threat Tree.

Por fim, é importante observar que 99 dos estudos analisados possuem um framework ou modelo como resultado final que pode ser utilizado como ferramenta para a etapa de engenharia de requisitos total ou parcial, no contexto de privacidade. A Tabela 3.6 apresenta o escopo dos frameworks/modelos encontrados nos estudos e suas respectivas referências.

RQ.1 Sumário: As técnicas mais utilizadas na Engenharia de Requisitos incluem SQUARE, Secure Tropos, PriS, I* (I-Star), LINDDUN, STRAP e Privacy by Design. Além dessas, alguns estudos desenvolveram novos frameworks e métodos baseados em abordagens existentes, demonstrando sua replicabilidade e usabilidade em diferentes contextos.

Escopo do Framework/Modelo	ID do Estudo
Requisitos de Privacidade em IoT	[PS41], [PS59]
Noções de Privacidade	[PS42], [PS44], [PS105], [PS11], [PS85]
Análise de Requisitos e Ameaças a Privacidade	[PS43], [PS51], [PS122], [PS63], [PS11], [PS112], [PS21], [PS80], [PS121], [PS82]
Elicitação de Requisitos de Privacidade	[PS103], [PS45], [PS1], [PS5], [PS106], [PS55], [PS58], [PS60], [PS9], [PS61], [PS10], [PS109], [PS12], [PS68] [PS69], [PS14], [PS111], [PS15], [PS113], [PS19], [PS114], [PS115], [PS34], [PS91], [PS92], [PS95], [PS96], [PS97], [PS98], [PS100], [PS33], [PS90], [PS89], [PS31], [PS87], [PS84], [PS117], [PS28], [PS27], [PS26]
Alinhamento de Requisitos de Segurança e Privacidade	[PS47], [PS4], [PS50], [PS23], [PS38], [PS40], [PS99], [PS32]
PriS	[PS2], [PS3], [PS6], [PS108], [PS124], [PS81]
COPri	[PS53], [PS54]
Privacy By Design, RBAC, PRET, P-STORE, Privacy-Enhanced BPMN (PE-BPMN), EPICUREAN, Secure Tropos, STRAP, TrUStAPIS	[PS56], [PS123], [PS66], [PS67], [PS125], [PS16], [PS74], [PS77], [PS24]
Conformidade com Legislações de Privacidade	[PS73], [PS78], [PS22], [PS118], [PS119], [PS36], [PS120], [PS93], [PS94], [PS39], [PS88], [PS86], [PS30], [PS25]
Requisitos de Privacidade em Blockchain	[PS17]
Requisitos de Privacidade no Metaverso	[PS76]

Tabela 3.6: Frameworks/Modelos Identificados nos Estudos

3.2.2 RQ.2. Quais as técnicas, métodos, processos, frameworks e ferramentas utilizadas na indústria para realizar o levantamento, análise, especificação, validação e gerenciamento dos requisitos de privacidade em diferentes contextos?

Para responder a esta pergunta, foi realizado um survey com os profissionais da área de privacidade para entender se as técnicas, métodos, processos, frameworks e ferramentas em Engenharia de Requisitos (ER) comumente descritas na literatura para a elicitação, análise, especificação, validação e gerenciamento de requisitos de privacidade são conhecidas ou utilizadas por profissionais. Utilizou-se a plataforma Google Forms para criar o questionário da pesquisa. Foi conduzida uma rodada de teste piloto para avaliar a qualidade da pesquisa, onde o questionário foi enviado para três profissionais que trabalham na área de privacidade. Seus comentários incluíram sugestões sobre a formulação das perguntas, exclusão de perguntas repetidas, alteração de alguns intervalos de tempo e alteração/inclusão de algumas opções de resposta, observações que foram levadas em consideração e os devidos ajustes foram realizados. Os entrevistados piloto levaram cerca de 10 minutos para concluir o questionário. Esse tempo foi relatado quando o questionário da pesquisa foi tornado público.

O survey consistiu em 16 perguntas: 15 fechadas e 1 aberta, conforme apresentado na Tabela 3.7. No início do survey, foi incluída uma declaração de consentimento informado e descrevendo os termos e condições.

Tabela 3.7: Questões do Survey

ID	Questão
Q1	Selecione o seu estado de atuação
Q2	Qual a sua idade?
Q3	Qual o seu nível de formação?
Q4	Há quanto tempo você trabalha na área de TIC (Tecnologia da Informação e Comunicação)?
Q5	Qual é a área de atuação da organização em que você participa/participou em um projeto de desenvolvimento de software?
Q6	Qual papel que melhor descreve suas atividades atuais em projetos de desenvolvimento de software?
Q7	Você trabalha ou já trabalhou no desenvolvimento de funcionalidades de um software que possuísse preocupações relacionadas a privacidade de dados?
Q8	A minha organização implementou ou está implementando mudanças devido a LGPD?

ID	Questão
Q9	O meu conhecimento sobre a Lei Geral de Proteção de dados (LGPD), que foi implementada em 2020, é suficiente para o desenvolvimento das minhas atividades nos projetos que estou participando?
Q10	Quais dos princípios da Lei Geral de Proteção de dados (LGPD) você conhece?
Q11	Quais dos princípios da LGPD a sua organização utiliza/implementa?
Q12	Com quais técnicas, métodos, processos, frameworks e ferramentas você já trabalhou ou trabalha atualmente?
Q13	Em qual fase da Engenharia de Requisitos você usa essas técnicas, métodos, processos, frameworks e ferramentas para lidar com os requisitos de privacidade?
Q14	Selecione as ferramentas utilizadas pela sua equipe de desenvolvimento de software para elicitar e documentar os requisitos de privacidade?
Q15	Você poderia descrever quais são os desafios que você ou sua equipe enfrentam para elicitar os requisitos de privacidade?

A pesquisa foi anônima e nenhuma informação de contato foi solicitada dos participantes. Em seguida, a pesquisa foi disponibilizada em várias plataformas de mídia social, incluindo LinkedIn, Facebook e Instagram. O questionário ficou aberto de 1º a 28 de novembro de 2024, por um total de 28 dias. No total, 37 profissionais responderam à pesquisa, onde as perguntas e opções de resposta foram disponibilizadas no Zenodo). A maioria dos participantes é da região Centro-Oeste (32 participantes) e tem mais de 4 anos de experiência em desenvolvimento de software (21 participantes), trabalhando como programadores/desenvolvedores. A Tabela 3.8 apresenta os perfis dos participantes. Setenta e um por cento (70.3%) dos participantes relataram que trabalharam ou estão trabalhando no desenvolvimento de recursos de software que envolvem preocupações com privacidade de dados. No entanto, 29.7% dos participantes declararam que não (Q7). Também houve 89.2% dos participantes que “concordam fortemente"ou “concordam"que sua organização implementou ou está em processo de implementação de mudanças devido à Lei Geral de Proteção de Dados (LGPD) brasileira (Q8). Além disso, 72.9% declararam que seu conhecimento da LGPD, que foi promulgada em 2020, é suficiente para realizar suas atividades nos projetos em que estão envolvidos. No entanto, 16.2%relataram que não têm o conhecimento necessário para implementar a LGPD (Q9) (Figura 3.6).

Também foi investigado quais princípios da LGPD os participantes estavam familiarizados (Q10). Os princípios mais conhecidos são segurança, qualidade de dados, transparência e propósito, conforme mostrado na Figura 3.7. Essa descoberta é semelhante à

REgião	#	%
Sudeste	3	8.1
Centro-Oeste	33	89.2
Sul	1	2.7
Faixa Etária	#	%
21 a 25 anos	11	29.7
26 a 30 anos	4	10.8
31 a 36 anos	2	5.4
37 a 42 anos	5	13.5
43 a 47 anos	7	18.9
48 a 54 anos	6	16.2
61 anos ou mais	2	5.4
Nível de Formação	#	%
Estudante de Graduação	7	18.9
Graduação	4	10.8
Especialização	5	13.5
Estudante de Mestrado	12	32.4
Mestrado	3	8.1
Estudante de Doutorado	4	10.8
Doutorado	2	5.4
Experiência	#	%
>=1 anos	4	10.8
Entre 1 e 3 anos	5	13.5
Entre 4 e 6 anos	7	18.9
Entre 7 e 10 anos	2	5.4
Entre 11 e 15 anos	3	8.1
Entre 16 e 20 anos	6	16.2
Mais de 21 anos	10	27
Área de Atuação	#	%
Administração pública federal	17	45.9
Administração pública estadual	7	18.9
Empresa privada de desenvolvimento de software	10	27
Projetos de colaboração/pesquisa	3	8.1
Cargo	#	%
Programador/Desenvolvedor	25	67.5
Engenheiro de Requisitos	3	8.1
Encarregado de Dados	4	10.8
Outros	5	13.51

Tabela 3.8: Demografia dos entrevistados da pesquisa (n= 37).

identificada em [5] e [4], onde os participantes do estudo também relataram estar mais familiarizados com esses princípios.

Em relação aos princípios da LGPD que as organizações dos participantes utilizam ou implementam (Q11), os praticantes afirmaram que os princípios mais utilizados e implementados em suas organizações são: Segurança (86.5%), Qualidade dos Dados (75.7%),

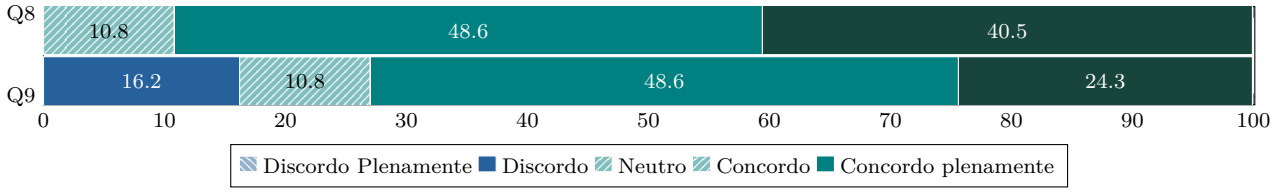


Figura 3.6: Percepções dos profissionais sobre como sua organização se adaptou à LGPD (Q8) e sua compreensão individual dos requisitos da lei no contexto de suas atividades diárias de projeto (Q9).

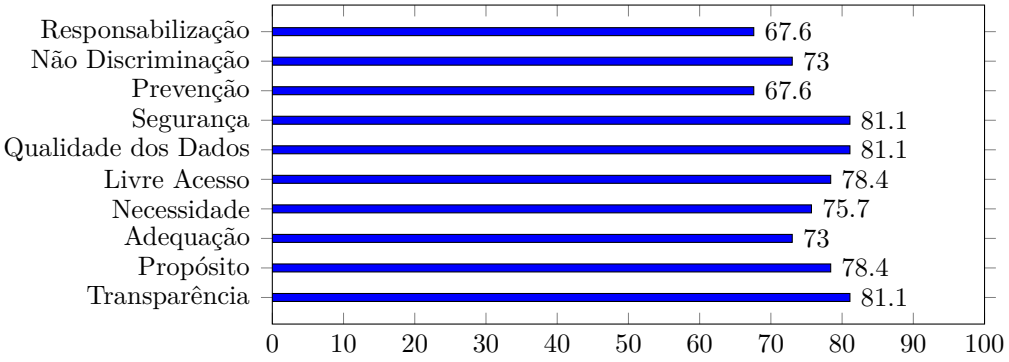


Figura 3.7: Princípios da LGPD conhecidos pelos participantes

Finalidade (75.5%), and Transparência (67.6%). O artigo [5] também identificou que os princípios de segurança e propósito foram os mais implementados pelos praticantes.

Em relação às técnicas, métodos, processos, frameworks e ferramentas com as quais os profissionais trabalharam ou trabalham atualmente (Q12), apenas 10 participantes relataram ter trabalhado com Privacy by Design e, desses, apenas alguns mencionaram ter trabalhado com ISO 29100 e SQUARE. Portanto, a maioria dos profissionais não usa as técnicas identificadas na literatura. Curiosamente, as descobertas diferem daquelas de [4], onde vários profissionais relataram usar Pris, NFR, RBAC, PbD, PCM e PET.

Em relação à fase onde os profissionais de Engenharia de Requisitos usam técnicas, métodos, processos, estruturas e ferramentas para abordar os requisitos de privacidade, a maioria deles relatou que é durante a fase de análise de requisitos (56.8%) e a fase de especificação (45.9%), como ilustrado na Figura 3.8.

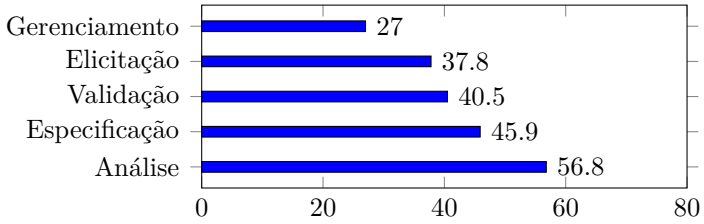


Figura 3.8: Técnicas por Fase de Engenharia de Requisitos

Em relação às ferramentas usadas pela equipe de desenvolvimento de software para obter e documentar requisitos de privacidade (Q14), a maioria dos participantes relatou não usar nenhuma ferramenta. No entanto, 4 participantes declararam que usam SMaRT e 2 participantes relataram usar PRIS, Strap e SPARQL, respectivamente. Essa descoberta é semelhante às descobertas de [63].

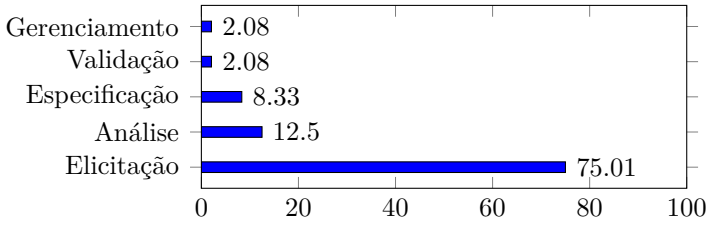
Em relação aos desafios que os profissionais enfrentam para obter requisitos de privacidade, #P19 disse: "As leis de privacidade podem mudar, e é essencial que os requisitos de privacidade estejam sempre alinhados com as regulamentações mais atuais. Além disso, em sistemas sensíveis ao contexto (como IoT), a coleta e o uso de dados aumentam a necessidade de requisitos de privacidade específicos, pois esses sistemas geralmente precisam lidar com informações pessoais confidenciais."; e #P28 disse: "A ausência de uma equipe dedicada para lidar com questões de privacidade de dados é o maior desafio enfrentado pela minha equipe".

RQ.2 Sumário: No geral, é possível observar que o uso de técnicas, métodos, processos, frameworks e ferramentas na indústria em muito se difere dos resultados encontrados a partir da academia. Pôde-se observar que os participantes da survey possuem grandes conhecimentos sobre os princípios da LGPD, juntamente com conhecimentos sobre o processo de Engenharia de Requisitos, mas não utilizam ou não conhecem uma grande quantidade de ferramentas desenvolvidas para o auxílio da elicitação de requisitos de privacidade.

3.2.3 RQ.3. Como as técnicas, métodos, processos, frameworks e ferramentas identificadas na literatura e na indústria são usadas nas fases da engenharia de requisitos?

De todos os 125 estudos selecionados, 48 focaram em etapas específicas da engenharia de requisitos, assim como ilustrado na Figura 3.9, comprovando um foco na etapa de elicitação de requisitos, o que foi possível observar também com base nos estudos que obtiveram Frameworks/Modelos como resultados finais, apresentados anteriormente na Tabela 3.6, onde a maior quantidade de resultados se concentra na etapa de elicitação de requisitos. Adicionalmente, a Tabela 3.9 apresenta os estudos com os respectivos focos nas fases da Engenharia de Requisitos.

Considerando a etapa de elicitação, os estudos [PS53] e [PS54] apresentam o desenvolvimento da ontologia COPri e COPri v.2, respectivamente. Os estudos focam no desenvolvimento de aperfeiçoamento desta ontologia criada para abordar a falta de compreensão dos engenheiros de requisitos em relação à necessidades específicas de privacidade,



Elicitação: 36 | Análise: 6 | Gerenciamento: 1 | Especificação: 4 | Validação: 1

Figura 3.9: Quantidade de Estudos por Etapa da Engenharia de Requisitos

Fase da ER	Referência
Elicitação	[PS6], [PS108], [PS81], [PS2], [PS5], [PS66], [PS42], [PS47], [PS3], [PS61], [PS52], [PS71], [PS75], [PS19], [PS4], [PS7], [PS65], [PS49], [PS70], [PS112], [PS16], [PS23], [PS53], [PS20], [PS24], [PS51], [PS54], [PS67], [PS9], [PS1], [PS48], [PS55], [PS10], [PS18], [PS22], [PS99]
Análise	[PS77], [PS15], [PS8], [PS21], [PS11], [PS125]
Especificação	[PS13], [PS73], [PS107], [PS12]
Validação	[PS104]
Gerenciamento	[PS14]

Tabela 3.9: Estudos Relacionados com as Fases da Engenharia de Requisitos

diferenciando-as de outros tipos de requisitos, como segurança. A ontologia fornece um conjunto genérico e expressivo de conceitos e relações chave relacionados à privacidade, como o consentimento fornecido pelos titulares dos dados, além da avaliação de riscos e tratamento de ameaças à privacidade, como anonimização e minimização de dados.

Para a etapa de validação, o processo SQUARE, apresentado anteriormente pelo estudo [PS104], permite a identificação de modificações necessárias para atender aos requisitos de privacidade na etapa de engenharia de requisitos.

Na etapa de especificação, destaca-se a metodologia LINDDUN, apresentada por [PS43] e incrementada por [PS107], onde são apresentados diversos requisitos e possíveis ameaças à privacidade, categorizados nas 7 categorias da metodologia, facilitando o processo de especificação de requisitos.

Na etapa de análise, destacam-se os frameworks apresentados em [PS43], [PS51], [PS122], [PS63], [PS112], [PS21], [PS80], juntamente de [PS11], que apresenta uma ferramenta para modelagem e análise de requisitos que incluem requisitos de privacidade, segurança e confiança, apresentando funcionalidade que minimizam os esforços de desenvolvedores de sistemas.

Focando na etapa de gestão de requisitos, o estudo [PS14] apresenta uma ferramenta

criada para suporte de Sistemas Ciberfísicos (CPS), onde o framework visa aprimorar o controle do usuário e a transparência no gerenciamento de privacidade, permitindo a execução automatizada de modelos de comportamento e validando o comportamento de tempo de execução do modelo DT, o que facilita o gerenciamento de privacidade eficaz por meio do compartilhamento transparente de autonomia entre os componentes CPS envolvidos.

Há um destaque também para o estudo [PS7], que propõe o conceito de "Early Privacy", sugerindo considerar a privacidade como um valor fundamental em todas as fases do projeto e desenvolvimento de sistemas. Utilizando um método de elicitação de requisitos de privacidade no contexto de sistemas de computação ubíqua, o estudo utiliza técnicas de desenvolvimento de questionários, personas, cenários e prototipações em design participativo para garantir que os requisitos de privacidade sejam alinhados com os modelos mentais dos usuários.

RQ.3 Summary: Analisando os estudos aceitos ao longo da revisão sistemática, foi possível observar um grande foco na etapa de elicitação, com diversos frameworks apresentados na Tabela 3.6, juntamente das metodologias apresentadas na resposta da questão de pesquisa RQ.1. Entretanto, embora exista uma grande quantidade de técnicas, métodos, processos, frameworks e ferramentas focada na etapa de elicitação de requisitos, entende-se que é igualmente necessário que exista também um foco nas outras etapas, principalmente nas etapas de gestão, validação e especificação, uma vez que todas as etapas possuem igual importância na engenharia de requisitos e principalmente na conformidade com requisitos de privacidade.

3.2.4 RQ.4. Quais são os desafios para elicitar os requisitos de privacidade?

Grande parte dos estudos analisados apresentam dificuldades e desafios de elicitação da requisitos de privacidade, entretanto, foi possível perceber um padrão nas dificuldades apresentadas, tanto na elicitação de requisitos de privacidade, quanto na aplicação destes requisitos em softwares. As principais dificuldades verificadas foram: aumento na complexidade do desenvolvimento de softwares e na fase de engenharia de requisitos, conflitos diretos com requisitos de segurança e alguns casos isolados afirmam o conflito direto de requisitos de privacidade com a natureza do software a ser desenvolvido. É importante notar que, poucos estudos comentaram e apresentaram dificuldades sobre os conflitos dos requisitos de privacidade com os requisitos de segurança, mas esse tema ainda foi conside-

rado relevante, uma vez que, de acordo com os artigos analisados, não existe ainda uma clara resposta para a resolução deste conflito.

Aumento na Complexidade do Desenvolvimento de Software

A maioria dos estudos mencionaram que o principal desafio em lidar com os requisitos de privacidade na etapa de engenharia de requisitos consistia no aumento da complexidade das atividades realizadas nesta etapa, devido a diversos fatores, tais como dificuldade de compreensão por parte dos engenheiros de requisitos e stakeholders dos requisitos de privacidade e de como aplicá-los na prática, assim como a dificuldade em compreender as legislações e normas de privacidade de dados existentes.

[PS1], [PS42], [PS44], [PS61], [PS68], [PS18], mencionaram que um dos fatores que contribuem para o aumento da complexidade do desenvolvimento de software está relacionado a dificuldade de compreensão e de conhecimento sobre os requisitos de privacidade. Os autores destacaram que existe uma carga adicional necessária de conhecimento sobre as leis de privacidade para os desenvolvedores ao lidar com esse tipo de requisitos, além de existir um engajamento menor por parte dos membros das equipes de desenvolvimento para tratar de problemas relacionados aos requisitos de privacidade, seja pela complexidade dos requisitos de privacidade ou pela falta de ferramentas adequadas para lidar com eles.

[PS102] and [PS10] também destacaram que o tratamento dos requisitos de privacidade pode comprometer a agilidade do processo de desenvolvimento. [PS102] investigaram os desafios dos times de software ágil para lidar com os requisitos de privacidade e sugeriram que as equipes de desenvolvimento usassem checklists com o uso de uma linguagem simples, para discutir e apresentar os requisitos de privacidade às partes interessadas, o que pode mitigar o efeito negativo na agilidade da equipe. [PS10] sugeriram que as equipes ágeis usem ferramentas automatizadas para fazer a revisão dos requisitos de privacidade.

[PS5] destacou que é necessário utilizar uma metodologia eficiente na fase de engenharia de requisitos para tratar os requisitos de privacidade, uma vez que lidar com esse tipo de requisitos é complexo em relação ao prazo para executar as atividades da ER e requer practitioners que estão acostumados a lidar com as leis de privacidade de dados, bem como com as técnicas existentes para garantir a privacidade. [PS52] and [PS22] também reportaram sobre a dificuldade dos practitioners em lidar com os conceitos complexos encontrados nas legislações e políticas de privacidade de dados. Adicionalmente, [PS60] investigou sobre como requisitos de privacidade podem ser vistos como vagos e desconexos da tecnologia, o que também contribui para o aumento da complexidade e desafios para a implementação desses requisitos na prática.

Tendo em vista os diferentes tipos de abordagens existentes para lidar com os requisitos de privacidade, [PS8] discutiram a importância de escolher uma abordagem correta para lidar com os requisitos de privacidade em diferentes contextos. Os autores destacaram que é necessário saber escolher entre abordagens como "privacy-by-policy" e "privacy-by-architecture", uma vez que a escolha errada de práticas de privacidade robustas pode gerar custos de desenvolvimento adicionais e complexidades desnecessárias. [PS78] também abordou o desafio de escolher a melhor abordagem para tratar os requisitos de privacidade e sugeriu que as partes interessadas (stakeholders) devem conduzir uma analise aprofundada dos prós e contras das diferentes estratégias de privacidade de dados existentes apresentada pelas equipes de desenvolvimento de software.

Os estudos [PS57] e [PS48] recomendaram que as equipes de desenvolvimento explorem a possibilidade de automação da atividade de elicitação de requisitos, aplicando técnicas de processamento de linguagem natural (NLP) para identificar não apenas os requisitos de privacidade, como também de requisitos de segurança. Adicionalmente, o estudo [PS71] sugeriu que seja desenvolvidos novos modelos de requisitos de privacidade, apresentando também a necessidade de uma incorporação de uma visão aprofundada de privacidade, levando em consideração conceitos mais complexos como privacidade de localização e atributos derivados probabilisticamente.

Requisitos de Privacidade X Requisitos de Segurança

Uma pequena quantidade dos estudos analisados: [PS43], [PS103] , [PS45], [PS47], [PS54], [PS23] [PS23], [PS99] relataram dificuldades na integração entre os requisitos de privacidade e requisitos de segurança, uma vez que, por mais que ambos possuam como objetivo primário a proteção dos dados, é possível observar que seus conceitos fundamentais divergem e, eventualmente, entram em conflito na fase de engenharia de requisitos. A maioria dos estudos apenas apresentaram as dificuldades e sugeriram pesquisas futuras na área para mitigação de conflitos. Entretanto, os estudos [PS47], [PS23], propuseram abordagens para mitigar e resolver os conflitos entre requisitos de privacidade e de segurança.

O estudo E83, de Alkubaisy *et al.* [PS23], mencionou as dificuldades e conflitos entre requisitos de privacidade e segurança, dando um destaque especial para os requisitos de Anonimização e Inobservabilidade (requisitos de privacidade que tratam do uso de recursos por parte de uma entidade sem que exista a revelação de sua identidade). Os autores afirmaram que estes dois requisitos apresentam uma maior quantidade de conflitos com outros requisitos de segurança, uma vez que estão diretamente ligados a não identificação de indivíduos dentro de um serviço, entrando diretamente em conflito, principalmente com os requisitos de Responsabilidade e Auditoria (requisitos de segurança que apresentam a necessidade de rastreamento de atividades de uma entidade, juntamente do requerimento

de vínculo de uma entidade às suas ações). Os autores propuseram a solução desses e de outros conflitos através da identificação de ferramentas que podem abranger um ou mais requisitos de privacidade e segurança ao mesmo tempo, identificando a necessidade de avaliação das ferramentas apresentadas em diferentes contextos para um melhor aproveitamento e desempenho.

Analogamente, Mouratidis *et al.* [PS47] destacaram a necessidade de um framework automatizado para dar suporte as equipes de desenvolvimento de software na modelagem do relacionamento dos requisitos de privacidade e de segurança. Os autores apresentaram o desenvolvimento inicial de um framework que pode auxiliar os desenvolvedores a realizar a elicitação dos requisitos de privacidade e segurança nas fases iniciais do processo de desenvolvimento de software.

Por mais que outros estudos apresentem aspectos conflitantes entre requisitos de privacidade e de segurança, [PS101] apresenta uma visão onde ambos os requisitos se sobrepõem parcialmente, embora não sejam idênticos. O estudo apresenta duas interpretações principais: a primeira se referindo a privacidade como um subconjunto de segurança, devido o fato de algumas medidas de segurança protegerem diretamente a privacidade. E a segunda interpretação apresenta estes dois conceitos como paralelos e com propósitos distintos, onde a segurança foca na resiliência técnica e organizacional de sistemas e a privacidade se refere ao uso ético e legítimo das informações pessoais.

Outros Desafios

Alguns estudos mencionaram desafios em contextos específicos que, por mais que não apresentem um problema generalizado, como o aumento de complexidade nas fases da engenharia de requisitos e desenvolvimento de software, ainda apresentam problemas significativos em suas respectivas áreas de conhecimento.

[PS41] apresentaram os desafios ao lidar com os requisitos de privacidade no contexto de Internet das Coisas (IoT), destacando que os serviços neste contexto não funcionam corretamente sem a coleta de dados. O estudo apresentou uma possível solução para mitigar o problema, consistindo no fato de que os desenvolvedores devem confiar nos dados existentes ou em resultados de pesquisas auto coletadas para informar o design de interfaces de configuração de privacidade, o que implica na necessidade de um processo de design cuidadoso para abordar as questões de privacidade.

[PS49] informaram que é necessário a existência de modelos conceituais que ajudem na compreensão dos conceitos de privacidade apresentados pelo Regulamento Geral sobre a Proteção de Dados (GDPR) [7], uma vez que a definição de privacidade na legislação contribui para confusões relacionadas a que medidas precisam ser tomadas para garantir a privacidade dos dados dos usuários. [PS114] também destacaram que existem desafios

na interpretação dos princípios da GDPR, o que pode levar a uma ambiguidade em como os requisitos de privacidade podem ser integrados na engenharia de requisitos, o que pode gerar problemas em relação a garantir a conformidade com a lei.

Como uma forma de solução parcial para este problema, [PS70] apresentaram 13 padrões de controle de privacidade com soluções orientadas a problemas e baseadas em padrões para os requisitos técnicos apresentados pela GDPR [7]. Adicionalmente, o estudo [PS72] apresentou a identificação e consolidação de 393 requisitos que cobrem aspectos legais de privacidade, segurança e aceitação da tecnologia. Ainda no contexto da GDPR [7], [PS64] apresenta um tutorial de conformidade referente aos requisitos de transparência da GDPR [7], juntamente com uma explicação de seu vocabulário de privacidade de dados, facilitando a conformidade com a legislação.

Em relação a Lei Geral de Proteção de Dados (LGPD) [8]. [PS83] informa que, de um modo geral, é necessário uma divulgação maior de informações referentes a LGDP [8], tanto em questões referentes ao alcance de divulgação, quanto em quantidade de conteúdo, tendo em vista a importância desse conhecimento para a criação de uma cultura de privacidade sólida, o que também é tratado como necessidade no estudo realizado, uma vez que os autores apresentam a importância da implementação desta cultura, visando um melhor tratamento de dados pessoais, conscientização dos usuários e conformidade de empresas.

Adicionalmente [PS46] informa diferentes dificuldades relacionadas a compreensão de requisitos de privacidade no contexto de brinquedos inteligentes, apontando que a maioria dos usuários não compreendem sistemas de controle parental e avisos de permissão, juntamente de políticas de privacidade. O estudo informa a falta de normas específicas para brinquedos inteligentes, o que dificulta a tradução de legislações em requisitos de privacidade técnicos que sejam precisos.

RQ.4 Sumário: Embora existam avanços significativos em relação aos requisitos de privacidade, ainda existe uma grande dificuldade em implementar esses requisitos na prática, uma vez que, requisitos de privacidade geram um aumento significativo na complexidade do desenvolvimento de software e nas atividades da engenharia de requisitos. Além disso, existe conflito entre requisitos de privacidade e requisitos de segurança, bem como outros desafios gerados por condições específicas apresentadas por alguns estudos.

3.3 Catálogo de Metodologias de Requisitos de Privacidade

Como compilação dos resultados obtidos durante a Revisão Sistemática de Literatura (RSL), este estudo possui como resultado um catálogo online dos frameworks identificados na RSL, juntamente das principais abordagens utilizadas como referências nos 125 estudos selecionados. O catálogo completo pode ser acessado através do seguinte link: https://sites.google.com/view/privacyreqframeworks/initial-page.

Este catálogo foi criado através da plataforma Google Sites e apresenta todos os 99 frameworks identificados na Revisão Sistemática de Literatura (RSL). Os frameworks foram separados em 11 categorias diferentes, baseadas nos respectivos escopos, conforme apresentado na Tabela 3.6.

A página inicial do catálogo apresenta uma breve descrição de seu objetivo para contextualização e, então, introduz as principais abordagens utilizadas pelos estudos aceitos durante a etapa da RSL, sendo elas: SQUARE, Secure Tropos, PriS, i*, LINDDUN, STRAP e Privacy By Design, conforme apresentado na Figura 3.10. Em seguida, são apresentadas as seções contendo cada framework, criadas a partir dos respectivos escopos dos frameworks, como ilustrando na Figura 3.11. Vale ressaltar que decidiu-se por criar o catálogo em inglês, para que seu conteúdo seja mais acessível.

Adicionalmente, junto das seções dos escopos dos frameworks, também é apresentada a seção "Outras Abordagens" onde são apresentadas outras abordagens encontradas ao longo dos estudos selecionados, mas que não obtiveram grande foco, se comparadas com as principais abordagens mencionadas anteriormente. A seção contém os seguintes tópicos: KAOS, GBRAM, RBAC, STRIDE, PRIPARE, P-STORE, ISO 29100, Bellotti-Sellen Framework, Moffett-Nuseibeh Framework, SecTro, PCM, ConfIS, SepTA, Privacy Impact Assessment, Asia-Pacific Economic Cooperation Privacy Framework, NFR, OECD Privacy Statement Generator, NIST Framework.

É importante ressaltar que, para todos os 99 frameworks e para todas as abordagens contidas no catálogo, foram adicionadas breves informações que explicam seu respectivo propósito, juntamente de links de acesso para os respectivos artigos, livros, sites que apresentam a metodologia ou framework, onde deu-se preferência por utilizar o DOI para artigos e publicações como link de acesso e, para os casos onde não foi possível encontrar o DOI ou o conteúdo de interesse constituía em um documento online ou página web, utilizou-se a URL da página.

Por fim, o catálogo possui uma seção de informações chamada "About", que apresenta as motivações e metodologias utilizadas neste trabalho para a sua construção, juntamente

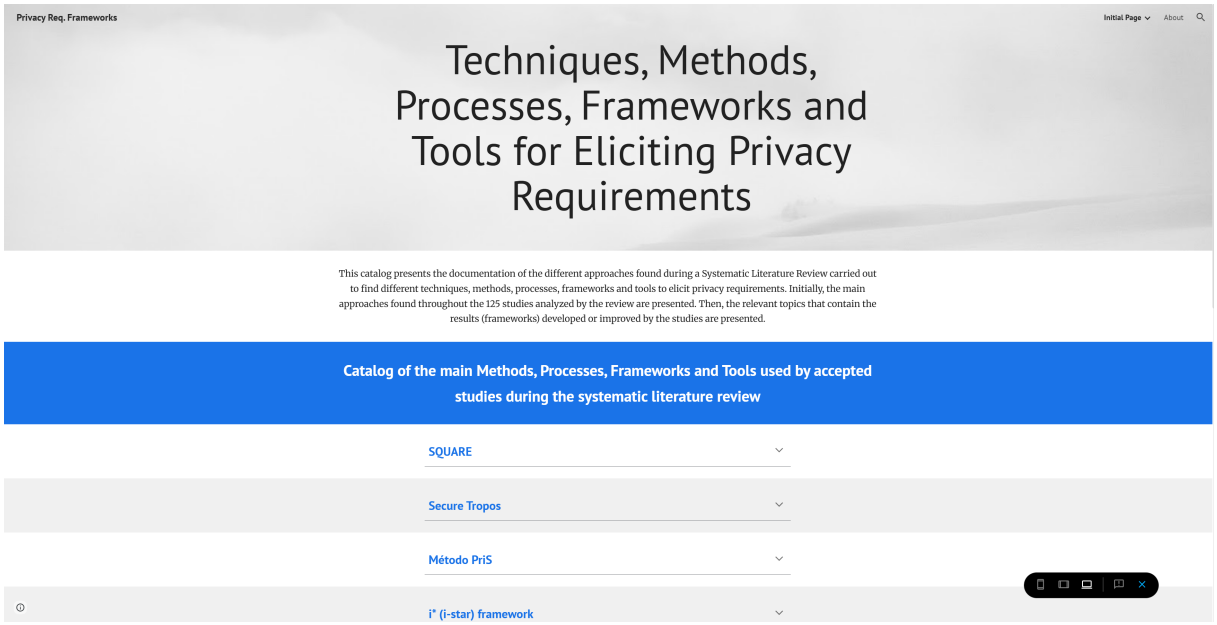


Figura 3.10: Página Inicial do Catálogo de Frameworks de Requisitos de Privacidade

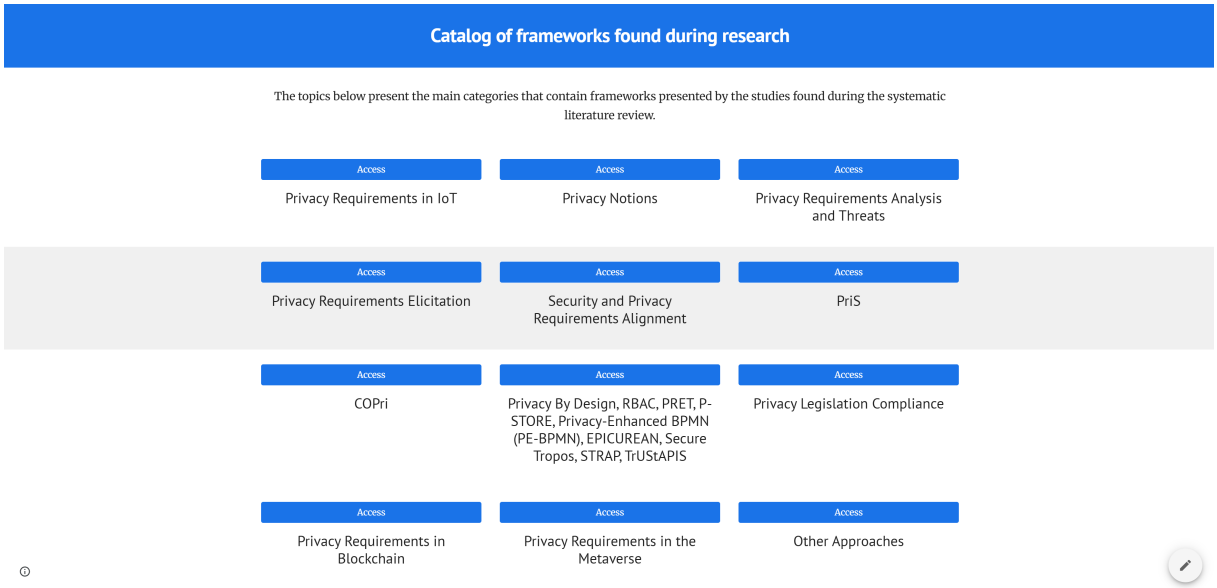


Figura 3.11: Categorias dos Frameworks

do link para o Zenodo com os artefatos resultantes da Revisão Sistemática de Literatura (RSL), como apresentado na Figura 3.12.

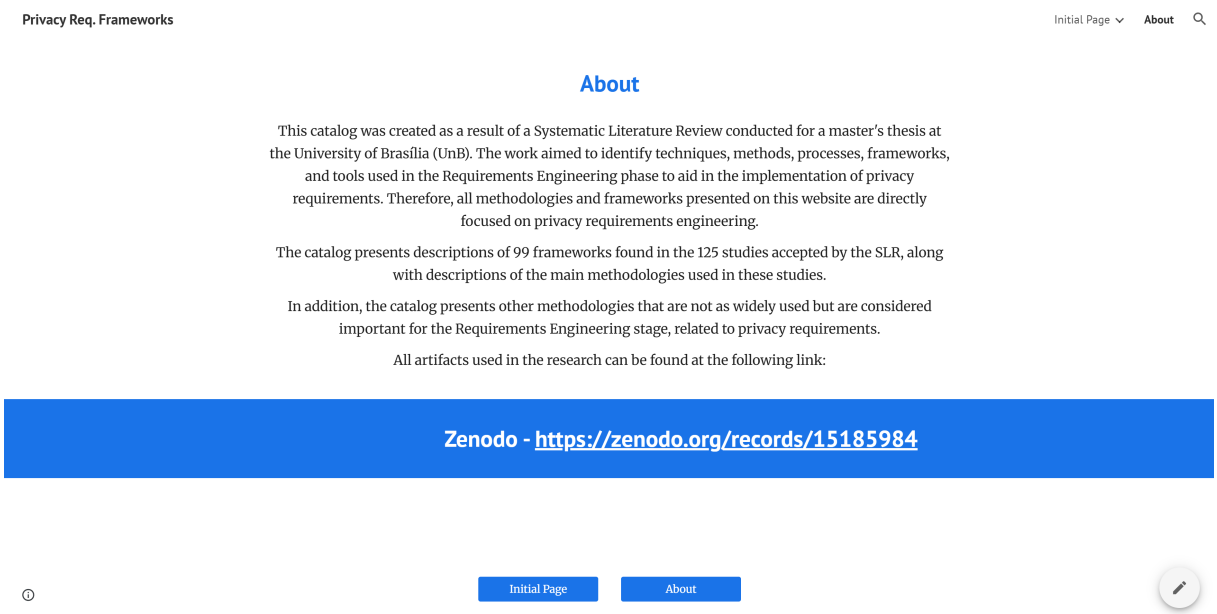


Figura 3.12: Página “About”

3.4 Discussões

3.4.1 Lacunas na Literatura e Pesquisas Futuras

Com base nos estudos analisados, foi possível observar que muitos sugerem a necessidade de aplicação de frameworks ou metodologias desenvolvidos em outros domínios além dos inicialmente abordados, como saúde, IoT e computação em nuvem, para validar a aplicabilidade dos resultados em contextos mais amplos. A maioria dos estudos destaca também a necessidade de estudos de caso mais amplos e robustos para validar as abordagens propostas em cenários reais e de grande escala, como sistemas nacionais de e-saúde, e em setores críticos como a cadeia de suprimentos farmacêutica.

É possível observar uma necessidade e demanda por ferramentas automatizadas que suportem a identificação, elicitação e análise de requisitos de privacidade, principalmente em ambientes utilizadores da metodologia Ágil e ambientes de computação em nuvem. Foi observado que alguns dos estudos analisados planejam desenvolver ou aprimorar ferramentas para facilitar a integração dos requisitos de privacidade em diferentes processos do desenvolvimento de software.

Adicionalmente, notou-se que a integração eficaz entre requisitos de segurança e privacidade é uma lacuna comum apresentada em diferentes estudos, com destaque para a necessidade de frameworks que abordem esses dois aspectos desde as fases iniciais de análise de requisitos até a implementação.

Ainda no contexto de lacunas identificadas, vários estudos mencionam dificuldades em tornar frameworks e ferramentas de privacidade acessíveis e compreensíveis tanto para

desenvolvedores quanto para usuários finais. Trabalhos futuros incluem a melhora da usabilidade de ferramentas apresentadas, simplificação de metodologias e investigação da eficácia da comunicação entre analistas e usuários.

Percebeu-se também que a falta de padronização é uma preocupação constante, especialmente em relação à adaptação dos métodos apresentados para diferentes legislações de privacidade, com um destaque especial para GDPR. Existe a necessidade da criação de frameworks mais generalizáveis e alinhados com os padrões legais de governança de privacidade. Também foi percebido a existência da necessidade de refinamento contínuo dos modelos e metodologias para acompanhar a evolução das regulamentações e tecnologias, incluindo o uso de machine learning para adaptação dos requisitos de privacidade.

3.5 Ameaças a Validade

As ameaças à validade deste estudo podem ser divididas em quatro categorias principais: construção, interna, externa e de conclusão [41]. Na validade de construção, a principal preocupação consiste na possível ambiguidade em definições de termos como "requisitos de privacidade" e "ferramentas", podendo variar entre estudos, além do possível risco dos critérios de inclusão e exclusão não capturem adequadamente todos os estudos relevantes. Para mitigar esses riscos, foram adotadas definições claras dos critérios de exclusão e aceitação, realizando calibrações ocasionais entre os pesquisadores para garantir a coerência dos critérios.

Em relação à validade interna, uma ameaça que pode ser considerada como padrão em todas as revisões sistemáticas de literatura, consiste no risco de viés na seleção de estudos e consequentemente de julgamentos subjetivos dos pesquisadores durante a extração de dados. Utilizando o guia de Kitchenham *et al.* [20], foi possível seguir uma série de diretrizes que minimizassem essa ameaça, sendo uma delas a seleção de bases recomendadas pelo próprio guia para fazer a busca de estudos. Adicionado a esse fator, a escolha de critérios de qualidades rigorosos contribuiu também para a mitigação dos riscos mencionados, tanto para as bases originalmente selecionadas, quanto para as bases utilizadas na busca manual realizada após a primeira etapa desta revisão.

No que tange à validade externa, a categorização de técnicas, métodos e ferramentas em subgrupos pode não capturar nuances entre abordagens similares, ou pode sobrepor categorias, dificultando a análise comparativa, uma vez que pequenas diferenças na metodologia ou aplicação podem gerar resultados que diferem entre ferramentas, por mais que estejam classificadas e categorizadas da mesma forma. Para lidar com essa questão, os critérios de extração foram definidos de forma que diferentes nuances, contextos e detalhes

pudessem ser extraídos para cada estudo analisado, permitindo um nível de diferenciação entre estudos e ferramentas que tratassem do mesmo tema e contexto.

Por fim, na validade de conclusão, a heterogeneidade dos estudos e a síntese qualitativa dos resultados podem introduzir subjetividade nas interpretações. Além disso, a evolução constante das regulamentações de privacidade e das tecnologias pode afetar a relevância dos achados ao longo do tempo. Em uma tentativa de mitigação das ameaças apresentadas nesse contexto, foi decidido um período de aceitação de estudos de até 20 anos atrás, mas com um foco maior em estudos dos últimos 10 anos, visando buscar técnicas da literatura que ainda são relevantes e utilizadas como base atualmente, mas também buscando metodologias inovativas e atuais. Além disso, buscou-se realizar uma classificação detalhada dos estudos encontrados e, assim, apresentar uma síntese de seus resultados, uma vez que foi entendido que uma síntese generalizada sobre os estudos encontrados não apresentaria informações nem qualidade relevantes para esta revisão de literatura.

Capítulo 4

Conclusão

Na revisão sistemática de literatura foram identificados 125 estudos primários que exploram diversas técnicas, métodos, processos, frameworks e ferramentas utilizadas na engenharia de requisitos para lidar com requisitos de privacidade. A revisão destacou que, embora exista uma ampla variedade de abordagens, a maioria das pesquisas está concentrada em contextos acadêmicos, com evidências limitadas de aplicação prática em larga escala na indústria. Abordagens amplamente utilizadas, como o Método PriS, Secure Tropos, LINDDUN, i* (i-star), STRAP, Privacy by Design (PbD) e SQUARE estão voltadas principalmente para a fase de elicitação dos requisitos de privacidade, indicando um foco significativo nas etapas iniciais da engenharia de requisitos. No entanto, a escassez de pesquisas dedicadas às fases posteriores — como análise, documentação, validação e gestão — apontam para uma necessidade urgente de maior investigação, a fim de garantir a integração completa dos requisitos de privacidade ao longo de todo o ciclo de vida do desenvolvimento de software.

Além disso, esta revisão identificou diversos desafios na elicitação de requisitos de privacidade, incluindo a crescente complexidade do desenvolvimento de software e a confusão entre requisitos de privacidade e de segurança. Esses desafios evidenciam a necessidade de abordagens integradas que consigam lidar de forma eficaz com as particularidades da privacidade no contexto das regulamentações de proteção de dados em constante evolução. Os resultados da pesquisa reforçam ainda mais esses desafios, revelando que, embora muitos profissionais estejam familiarizados com os princípios da LGPD e concordem que suas organizações estão se adaptando à regulamentação, a adoção de práticas estruturadas de engenharia da privacidade ainda é limitada. Métodos informais e a ausência de ferramentas durante a elicitação de requisitos de privacidade são comuns, refletindo a necessidade de maior conscientização, capacitação direcionada e recursos práticos para reduzir a lacuna entre o conhecimento teórico e a aplicação no mundo real.

Adicionalmente, foi desenvolvido um catálogo que contém as principais informações

a respeito dos frameworks encontrados nos estudos aceitos pela Revisão Sistemática de Literatura (RSL), juntamente de informações sobre as principais metodologias utilizadas nos respectivos estudos.

Por fim, entende-se que pesquisas futuras devem buscar preencher as lacunas identificadas, investigando a escalabilidade, adaptabilidade e eficácia dessas técnicas, métodos, processos, frameworks e ferramentas em diversos ambientes de software do mundo real. Esses esforços contribuirão para fortalecer as práticas de preservação da privacidade na fase de engenharia de requisitos e para o desenvolvimento de sistemas de software conscientes da privacidade, que atendam tanto às exigências regulatórias quanto às expectativas dos usuários.

References

[1] Cheng, Betty H.C. e Joanne M. Atlee: *Research directions in requirements engineering.* Em *Future of Software Engineering (FOSE '07)*, páginas 285–303, 2007. x, 12, 13

[2] Cheung, Muller Y. M. e Hao Liu: *Information privacy concerns in generative AI.* Em *Australasian Conference on Information Systems, ACIS 2023, Wellington, New Zealand, December 5-8, 2023*, 2023. https://aisel.aisnet.org/acis2023/24. 1, 3

[3] Golda, Abenezer, Kidus Mekonen, Amit Pandey, Anushka Singh, Vikas Hassija, Vinay Chamola e Biplab Sikdar: *Privacy and security concerns in generative AI: A comprehensive survey.* IEEE Access, 12:48126–48144, 2024. https://doi.org/10.1109/ACCESS.2024.3381611. 1, 2, 3

[4] Canedo, Edna Dias, Ian Nery Bandeira, Angélica Toffano Seidel Calazans, Pedro Henrique Teixeira Costa, Emille Catarine Rodrigues Cançado e Rodrigo Bonifácio: *Privacy requirements elicitation: a systematic literature review and perception analysis of IT practitioners.* Requir. Eng., 28(2):177–194, 2023. https://doi.org/10.1007/s00766-022-00382-8. 1, 2, 3, 12, 14, 42, 43

[5] Canedo, Edna Dias, Angélica Toffano Seidel Calazans, Anderson Jefferson Cerqueira, Pedro Henrique Teixeira Costa e Eloisa Toffano Seidel Masson: *Agile teams' perception in privacy requirements elicitation: Lgpd's compliance in brazil.* Em *29th IEEE International Requirements Engineering Conference, RE 2021, Notre Dame, IN, USA, September 20-24, 2021*, páginas 58–69. IEEE, 2021. https://doi.org/10.1109/RE51729.2021.00013. 1, 42, 43

[6] Amorim, Joni A., Rose-Mharie Åhlfeldt, Per M. Gustavsson e Sten F. Andler: *Privacy and security in cyberspace: Training perspectives on the personal data ecosystem.* Em *2013 European Intelligence and Security Informatics Conference, Uppsala, Sweden, August 12-14, 2013*, páginas 139–142, https://dblp.org/rec/conf/eisic/AmorimAGA13.bib, 2013. https://doi.org/10.1109/EISIC.2013.30. 1

[7] Parliament, The European e The Council: *General Data Protection Regulation (GDPR).* Intersoft Consulting, 2018. https://gdpr-info.eu. 1, 2, 7, 8, 9, 25, 49, 50

[8] Brasil: *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, 2018. http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. 1, 7, 9, 10, 25, 50

[9] Westin, Alan F: *Privacy and freedom*. Washington and Lee Law Review, 25(1):166, 1968. 2

[10] Pfleeger, Charles P. e Shari Lawrence Pfleeger: *Security in Computing*. Prentice Hall Professional Technical Reference, 3rd edição, 2002, ISBN 0130355488. 2

[11] Radics, Peter J., Denis Gracanin e Dennis G. Kafura: *Preprocess before you build: Introducing a framework for privacy requirements engineering*. Em *International Conference on Social Computing, SocialCom 2013, SocialCom/PASSAT/BigData/EconCom/BioMedCom 2013, Washington, DC, USA, 8-14 September, 2013*, páginas 564–569. IEEE Computer Society, 2013. https://doi.org/10.1109/SocialCom.2013.85. 2

[12] Li, Tong e Zhishuai Chen: *An ontology-based learning approach for automatically classifying security requirements*. J. Syst. Softw., 165:110566, 2020. https://doi.org/10.1016/j.jss.2020.110566. 2

[13] Radics, Peter J. e Denis Gracanin: *Privacy in domestic environments*. Em Tan, Desney S., Saleema Amershi, Bo Begole, Wendy A. Kellogg e Manas Tungare (editores): *Proceedings of the International Conference on Human Factors in Computing Systems, CHI 2011, Extended Abstracts Volume, Vancouver, BC, Canada, May 7-12, 2011*, páginas 1735–1740. ACM, 2011. https://doi.org/10.1145/1979742.1979837. 2

[14] Ferrão, Sâmmara Éllen Renner, Geovana Ramos Sousa Silva, Edna Dias Canedo e Fabiana Freitas Mendes: *Towards a taxonomy of privacy requirements based on the LGPD and ISO/IEC 29100*. Inf. Softw. Technol., 168:107396, 2024. 2, 11, 14

[15] Canedo, Edna Dias, Anderson Jefferson Cerqueira, Rogério Machado Gravina, Vanessa Coelho Ribeiro, Renato Camões, Vinicius Eloy dos Reis, Fábio Lúcio Lopes de Mendonça e Rafael T. de Sousa Jr.: *Proposal of an implementation process for the brazilian general data protection law (LGPD)*. Em Filipe, Joaquim, Michal Smialek, Alexander Brodsky e Slimane Hammoudi (editores): *Proceedings of the 23rd International Conference on Enterprise Information Systems, ICEIS 2021, Online Streaming, April 26-28, 2021, Volume 1*, páginas 19–30. SCITEPRESS, 2021. https://doi.org/10.5220/0010398200190030. 2

[16] Alkubaisy, Duaa, Karl Cox e Haralambos Mouratidis: *Towards detecting and mitigating conflicts for privacy and security requirements*. Em Kolp, Manuel, Jean Vanderdonckt, Monique Snoeck e Yves Wautelet (editores): *13th International Conference on Research Challenges in Information Science, RCIS 2019, Brussels, Belgium, May 29-31, 2019*, páginas 1–6. IEEE, 2019. https://doi.org/10.1109/RCIS.2019.8876999. 2

[17] Herwanto, Guntur Budi, Fajar J. Ekaputra, Gerald Quirchmayr e A Min Tjoa: *Toward a holistic privacy requirements engineering process: Insights from a systematic literature review*. IEEE Access, 12:47518–47542, 2024. https://doi.org/10.1109/ACCESS.2024.3380888. 2, 3, 12

[18] Miyazaki, Seiya, Nancy Mead e Justin Zhan: *Computer-aided privacy requirements elicitation technique*. Em *2008 IEEE Asia-Pacific Services Computing Conference*, páginas 367–372, 2008. 3

[19] Coles, Joshua, Shamal Faily e Duncan Ki-Aries: *Tool-supporting data protection impact assessments with cairis*. Em *2018 IEEE 5th International Workshop on Evolving Security & Privacy Requirements Engineering (ESPRE)*, páginas 21–27, 2018. 3

[20] Keele, Staffs *et al.*: *Guidelines for performing systematic literature reviews in software engineering*, 2007. 4, 16, 17, 20, 54

[21] Gharib, Mohamad, Paolo Giorgini e John Mylopoulos: *Towards an ontology for privacy requirements via a systematic literature review*. Em Mayr, Heinrich C., Giancarlo Guizzardi, Hui Ma e Oscar Pastor (editores): *Conceptual Modeling - 36th International Conference, ER 2017, Valencia, Spain, November 6-9, 2017, Proceedings*, volume 10650 de *Lecture Notes in Computer Science*, páginas 193–208. Springer, 2017. https://doi.org/10.1007/978-3-319-69904-2_16. 7

[22] Silva Junior, Deógenes P. da, Patricia Cristiane de Souza e Thaíres A. de Jesus Gonçalves: *Early privacy: Approximating mental models in the definition of privacy requirements in systems design*. Em Mota, Marcelle, Bianchi Serique Meiguins, Raquel O. Prates e Heloisa Candello (editores): *Proceedings of the 17th Brazilian Symposium on Human Factors in Computing Systems, IHC 2018, Belém, Brazil, October 22-26, 2018*, páginas 19:1–19:10. ACM, 2018. https://doi.org/10.1145/3274192.3274211. 7

[23] Veseli, Fatbardh, Jetzabel Serna-Olvera, Tobias Pulls e Kai Rannenberg: *Engineering privacy by design: lessons from the design and implementation of an identity wallet platform*. Em Hung, Chih-Cheng e George A. Papadopoulos (editores): *Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing, SAC 2019, Limassol, Cyprus, April 8-12, 2019*, páginas 1475–1483. ACM, 2019. https://doi.org/10.1145/3297280.3297429. 7

[24] Kalloniatis, Christos, Evangelia Kavakli e Stefanos Gritzalis: *Dealing with privacy issues during the system design process*. Em *Proceedings of the Fifth IEEE International Symposium on Signal Processing and Information Technology, 2005.*, páginas 546–551. IEEE, 2005. 8

[25] Tsohou, Aggeliki, Emmanouil Magkos, Haralambos Mouratidis, George Chrysoloras, Luca Piras, Michalis Pavlidis, Julien Debussche, Marco Rotoloni e Beatriz Gallego-Nicasio Crespo: *Privacy, security, legal and technology acceptance elicited and consolidated requirements for a gdpr compliance platform*. Information & Computer Security, 28(4):531–553, 2020. 8

[26] Lorenzon, Laila Neves: *Análise comparada entre regulamentações de dados pessoais no brasil e na união europeia (lgpd e gdpr) e seus respectivos instrumentos de enforcement*. Revista do Programa de Direito da União Europeia, 1:39–52, 2021. 8

[27] Li, He, Lu Yu e Wu He and: *The impact of gdpr on global technology development*. Journal of Global Information Technology Management, 22(1):1–6, 2019. https://doi.org/10.1080/1097198X.2019.1569186. 8

[28] Arfelt, Emma, David Basin e Søren Debois: *Monitoring the gdpr*. Em Sako, Kazue, Steve Schneider e Peter Y. A. Ryan (editores): *Computer Security – ESORICS 2019*, páginas 681–699, Cham, 2019. Springer International Publishing, ISBN 978-3-030-29959-0. 8

[29] Schlehahn, Eva e Rigo Wenning: *GDPR transparency requirements and data privacy vocabularies*. Em Kosta, Eleni, Jo Pierson, Daniel Slamanig, Simone Fischer-Hübner e Stephan Krenn (editores): *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 de *IFIP Advances in Information and Communication Technology*, páginas 95–113. Springer, 2018. https://doi.org/10.1007/978-3-030-16744-8_7. 8

[30] Rocha, Lucas Dalle, Geovana Ramos Sousa Silva e Edna Dias Canedo: *Privacy compliance in software development: A guide to implementing the lgpd principles*. Em *Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing*, SAC '23, página 1352–1361, New York, NY, USA, 2023. Association for Computing Machinery, ISBN 9781450395175. https://doi.org/10.1145/3555776.3577615. 9

[31] Alves, Carina e Moisés Neves: *Especificação de requisitos de privacidade em conformidade com a LGPD: resultados de um estudo de caso*. Em Menezes Cruz, Maria Lencastre Pinheiro de, Graciela Dora Susana Hadad e Johnny Cardoso Marques (editores): *Anais do WER21 - Workshop em Engenharia de Requisitos, Brasilia, BSB, Brasil, August 23-27, 2021*. Editora PUC-Rio, 2021. https://doi.org/10.29327/1298728.24-14. 10

[32] Frej, Matheus, Ivonildo Pereira Gomes Neto, Waldemar Ferreira e Sérgio Soares: *Um sistema web para auxiliar soluções na conformidade com a LGPD*. Em *Proceedings of the 38th Brazilian Symposium on Software Engineering, SBES 2024, Curitiba, Brazil, September 30 - October 4, 2024*, páginas 713–719, 2024. https://doi.org/10.5753/sbes.2024.3558. 11, 15

[33] Camêlo, Moisés Neves e Carina Alves: *G-priv: Um guia para apoiar a especificação de requisitos de privacidade em conformidade com a LGPD*. Braz. J. Inf. Syst., 16(1), 2023. https://doi.org/10.5753/isys.2023.2743. 11, 15

[34] Zave, Pamela: *Classification of research efforts in requirements engineering*. ACM Comput. Surv., 29(4):315–321, dezembro 1997, ISSN 0360-0300. https://doi.org/10.1145/267580.267581. 11, 12

[35] Bennaceur, Amel, Thein Than Tun, Yijun Yu e Bashar Nuseibeh: *Requirements Engineering*, páginas 51–92. Springer International Publishing, Cham, 2019, ISBN 978-3-030-00262-6. https://doi.org/10.1007/978-3-030-00262-6_2. 12

[36] Peixoto, Mariana Maia, Carla T. L. L. Silva, João Araújo, Tony Gorschek, Alexandre M. L. de Vasconcelos e Jéssyka Vilela: *Evaluating a privacy requirements specification method by using a mixed-method approach: results and lessons learned.* Requir. Eng., 28(2):229–255, 2023. https://doi.org/10.1007/s00766-022-00388-2. 12

[37] Notario, Nicolás, Alberto Crespo, Yod Samuel Martín, José M. del Álamo, Daniel Le Métayer, Thibaud Antignac, Antonio Kung, Inga Kroener e David Wright: *PRIPARE: integrating privacy best practices into a privacy engineering methodology.* Em *2015 IEEE Symposium on Security and Privacy Workshops, SPW 2015, San Jose, CA, USA, May 21-22, 2015*, páginas 151–158. IEEE Computer Society, 2015. https://doi.org/10.1109/SPW.2015.22. 12

[38] Hansen, Marit, Meiko Jensen e Martin Rost: *Protection goals for privacy engineering.* Em *2015 IEEE Symposium on Security and Privacy Workshops, SPW 2015, San Jose, CA, USA, May 21-22, 2015*, páginas 159–166. IEEE Computer Society, 2015. https://doi.org/10.1109/SPW.2015.13. 13, 14

[39] Caiza, Julio C., Yod Samuel Martín, Danny S. Guamán, José M. del Álamo e Juan C. Yelmo: *Reusable elements for the systematic design of privacy-friendly information systems: A mapping study.* IEEE Access, 7:66512–66535, 2019. https://doi.org/10.1109/ACCESS.2019.2918003. 14, 15

[40] Petersen, Kai, Sairam Vakkalanka e Ludwik Kuzniarz: *Guidelines for conducting systematic mapping studies in software engineering: An update.* Information and software technology, 64:1–18, 2015. 17

[41] Wohlin, Claes, Per Runeson, Martin Höst, Magnus C Ohlsson, Björn Regnell, Anders Wesslén, Claes Wohlin, Per Runeson, Martin Höst, Magnus C Ohlsson *et al.*: *Systematic literature reviews.* Experimentation in software engineering, páginas 45–54, 2012. 18, 54

[42] Hidellaarachchi, Dulaji, John Grundy, Rashina Hoda e Kashumi Madampe: *The effects of human aspects on the requirements engineering process: A systematic literature review.* IEEE Transactions on Software Engineering, 48(6):2105–2127, 2021. 25

[43] Castro, Jaelson, Manuel Kolp e John Mylopoulos: *A requirements-driven development methodology.* Em *Advanced Information Systems Engineering: 13th International Conference, CAiSE 2001 Interlaken, Switzerland, June 4–8, 2001 Proceedings 13*, páginas 108–123. Springer, 2001. 31

[44] Yu, E, L Liu e J Mylopoulous: *A social ontology for integrating security and software engineering.* Em *Integrating security and software engineering: Advances and future visions*, páginas 70–106. IGI Global, 2007. 32

[45] Cavoukian, Ann *et al.*: *Privacy by design: The seven foundational principles.* IAPP Resource Center, https://iapp. org/resources/article/privacy-by-design-the-7-foundational-principles, 2021. 34

[46] Van Lamsweerde, Axel, Anne Dardenne, Bruno Delcourt e Françoise Dubisy: *The kaos project: Knowledge acquisition in automated specification of software*. Em *Proceedings of the AAAI Spring Symposium Series*, 1991. 35

[47] Anton, A.I.: *Goal-based requirements analysis*. Em *Proceedings of the Second International Conference on Requirements Engineering*, páginas 136–144, 1996. 35

[48] Sandhu, Ravi S.: *Role-based access control11portions of this chapter have been published earlier in sandhu et al. (1996), sandhu (1996), sandhu and bhamidipati (1997), sandhu et al. (1997) and sandhu and feinstein (1994)*. Volume 46 de *Advances in Computers*, páginas 237–286. Elsevier, 1998. https://www.sciencedirect.com/science/article/pii/S0065245808602065. 36

[49] Microsoft: *The stride threat model*, 2009. 36

[50] Notario, Nicolas, Alberto Crespo, Yod Samuel Martin, Jose M. Del Alamo, Daniel Le Metayer, Thibaud Antignac, Antonio Kung, Inga Kroener e David Wright: *Pripare: Integrating privacy best practices into a privacy engineering methodology*. Em *2015 IEEE Security and Privacy Workshops*, páginas 151–158, 2015. 36

[51] Standardization, International Organization for: *ISO/IEC 29100:2024 — information technology — security techniques — privacy framework*, 2024. https://www.iso.org/standard/85938.html. 36

[52] Bellotti, Victoria e Abigail Sellen: *Design for privacy in ubiquitous computing environments*. Em *Third European Conference on Computer Supported Cooperative Work, ECSCW'93, Milano, Italy, September 13-17, 1993, Proceedings*, página 75. Kluwer Academic Publishers, 1993. 36

[53] Haley, Charles B., Jonathan D. Moffett, Robin C. Laney e Bashar Nuseibeh: *A framework for security requirements engineering*. Em Bruschi, Danilo, Bart De Win e Mattia Monga (editores): *Proceedings of the 2006 international workshop on Software engineering for secure systems, SESS 2006, Shanghai, China, May 20-21, 2006*, páginas 35–42. ACM, 2006. https://doi.org/10.1145/1137627.1137634. 37

[54] Pavlidis, Michalis e Shareeful Islam: *Sectro: A CASE tool for modelling security in requirements engineering using secure tropos*. Em Nurcan, Selmin (editor): *Proceedings of the CAiSE Forum 2011, London, UK, June 22-24, 2011*, volume 734 de *CEUR Workshop Proceedings*, páginas 89–96. CEUR-WS.org, 2011. https://ceur-ws.org/Vol-734/PaperDemo12.pdf. 37

[55] Peixoto, Mariana, Carla Silva, Ricarth Lima, Joao Araújo, Tony Gorschek e Jean Silva: *Pcm tool: Privacy requirements specification in agile software development*. Em *Congresso Brasileiro de Software: Teoria e Prática (CBSoft)*, páginas 108–113. SBC, 2019. 37

[56] Alkubaisy, Duaa, Luca Piras, Mohammed Ghazi Al-Obeidallah, Karl Cox e Haralambos Mouratidis: *Confis: A tool for privacy and security analysis and conflict*

resolution for supporting GDPR compliance through privacy-by-design. Em Ali, Raian, Hermann Kaindl e Leszek A. Maciaszek (editores): *Proceedings of the 16th International Conference on Evaluation of Novel Approaches to Software Engineering, ENASE 2021, Online Streaming, April 26-27, 2021*, páginas 80–91. SCITEPRESS, 2021. https://doi.org/10.5220/0010406100800091. 37

[57] Salnitri, Mattia, Konstantinos Angelopoulos, Michalis Pavlidis, Vasiliki Diamantopoulou, Haralambos Mouratidis e Paolo Giorgini: *Modelling the interplay of security, privacy and trust in sociotechnical systems: a computer-aided design approach*. Softw. Syst. Model., 19(2):467–491, 2020. https://doi.org/10.1007/s10270-019-00744-x. 37

[58] Wright, David: *The state of the art in privacy impact assessment*. Computer Law & Security Review, 28(1):54–61, 2012, ISSN 2212-473X. https://www.sciencedirect.com/science/article/pii/S026736491100183X. 37

[59] Cooperation, Asia Pacific Economic: *Apec privacy framework*. Asia Pacific Economic Cooperation Secretariat, 81, 2005. https://www.apec.org/publications/2005/12/apec-privacy-framework. 38

[60] Chung, Lawrence, Brian A. Nixon, Eric Yu e John Mylopoulos: *Non-Functional Requirements in Software Engineering*, volume 5 de *International Series in Software Engineering*. Springer, 2000, ISBN 978-1-4613-7403-9. https://doi.org/10.1007/978-1-4615-5269-7. 38

[61] OECD: *Making privacy notices simple: An oecd report and recommendations*. Relatório Técnico 120, OECD Publishing, Paris, 2006. https://doi.org/10.1787/231428216052. 38

[62] Standards, National Institute of e Technology: *The nist cybersecurity framework (csf)*, 2024. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf. 38

[63] Canedo, Edna Dias, Angélica Toffano Seidel Calazans, Ian Nery Bandeira, Pedro Henrique Teixeira Costa e Eloisa Toffano Seidel Masson: *Guidelines adopted by agile teams in privacy requirements elicitation after the brazilian general data protection law (LGPD) implementation*. Requir. Eng., 27(4):545–567, 2022. https://doi.org/10.1007/s00766-022-00391-7. 44

Primary Studies

[PS1] Sangaroonsilp, Pattaraporn, Hoa Khanh Dam, Morakot Choetkiertikul, Chaiyong Ragkhitwetsagul e Aditya Ghose: *A taxonomy for mining and classifying privacy requirements in issue reports*. Inf. Softw. Technol., 157:107162, 2023. https://doi.org/10.1016/j.infsof.2023.107162.

[PS2] Kalloniatis, Christos, Evangelia Kavakli e Stefanos Gritzalis: *Addressing privacy requirements in system design: the pris method*. Requirements Engineering, 13:241–255, 2008.

[PS3] Kalloniatis, Christos, Petros Belsis, Evangelia Kavakli e Stefanos Gritzalis: *Applying soft computing technologies for implementing privacy-aware systems*. Em *Advanced Information Systems Engineering Workshops: CAiSE 2012 International Workshops, Gdańsk, Poland, June 25-26, 2012. Proceedings 24*, páginas 31–45. Springer, 2012.

[PS4] Islam, Shareeful, Moussa Ouedraogo, Christos Kalloniatis, Haralambos Mouratidis e Stefanos Gritzalis: *Assurance of security and privacy requirements for cloud deployment models*. IEEE Transactions on Cloud Computing, 6(2):387–400, 2015.

[PS5] Miyazaki, Seiya, Nancy Mead e Justin Zhan: *Computer-aided privacy requirements elicitation technique*. Em *2008 IEEE Asia-Pacific Services Computing Conference*, páginas 367–372. IEEE, 2008.

[PS6] Kalloniatis, Christos, Evangelia Kavakli e Stefanos Gritzalis: *Dealing with privacy issues during the system design process*. Em *Proceedings of the Fifth IEEE International Symposium on Signal Processing and Information Technology, 2005.*, páginas 546–551. IEEE, 2005.

[PS7] Silva Junior, Deógenes P. da, Patricia Cristiane de Souza e Thaíres A. de Jesus Gonçalves: *Early privacy: Approximating mental models in the definition of privacy requirements in systems design*. Em Mota, Marcelle, Bianchi Serique Meiguins, Raquel O. Prates e Heloisa Candello (editores): *Proceedings of the 17th Brazilian Symposium on Human Factors in Computing Systems, IHC 2018, Belém, Brazil, October 22-26, 2018*, páginas 19:1–19:10. ACM, 2018. https://doi.org/10.1145/3274192.3274211.

[PS8] Spiekermann, Sarah e Lorrie Faith Cranor: *Engineering privacy*. IEEE Transactions on software engineering, 35(1):67–82, 2008.

[PS9] Peixoto, Mariana, Carla Silva, João Araújo, Tony Gorschek, Alexandre Vasconcelos e Jéssyka Vilela: *Evaluating a privacy requirements specification method by using a mixed-method approach: results and lessons learned*. Requirements Engineering, 28(2):229–255, 2023.

[PS10] Herwanto, Guntur Budi, Gerald Quirchmayr e A Min Tjoa: *Leveraging nlp techniques for privacy requirements engineering in user stories*. IEEE Access, 2024.

[PS11] Salnitri, Mattia, Konstantinos Angelopoulos, Michalis Pavlidis, Vasiliki Diamantopoulou, Haralambos Mouratidis e Paolo Giorgini: *Modelling the interplay of security, privacy and trust in sociotechnical systems: a computer-aided design approach*. Software and Systems Modeling, 19(2):467–491, 2020.

[PS12] Peixoto, Mariana, Carla Silva, Ricarth Lima, Joao Araújo, Tony Gorschek e Jean Silva: *Pcm tool: Privacy requirements specification in agile software development*. Em *Anais Estendidos do X Congresso Brasileiro de Software: Teoria e Prática*, páginas 108–113. SBC, 2019.

[PS13] Hörbe, Rainer e Walter Hötzendorfer: *Privacy by design in federated identity management*. Em *2015 IEEE Security and Privacy Workshops*, páginas 167–174. IEEE, 2015.

[PS14] Stary, Christian e Richard Heininger: *Privacy by sharing autonomy–a design-integrating engineering approach*. Em *International Conference on Subject-Oriented Business Process Management*, páginas 3–22. Springer, 2022.

[PS15] Kavakli, Evangelia, Stefanos Gritzalis e Kalloniatis Christos: *Protecting privacy in system design: the electronic voting case*. Transforming Government: People, Process and Policy, 1(4):307–332, 2007.

[PS16] Stach, Christoph e Frank Steimle: *Recommender-based privacy requirements elicitation-epicurean: an approach to simplify privacy settings in iot applications with respect to the gdpr*. Em *Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing*, páginas 1500–1507, 2019.

[PS17] Aslam, Sidra, Aleksandar Tošić e Michael Mrissa: *Secure and privacy-aware blockchain design: Requirements, challenges and solutions*. Journal of Cybersecurity and Privacy, 1(1):164–194, 2021.

[PS18] Zhao, Qingsong, Lei Shu, Kailiang Li, Mohamed Amine Ferrag, Ximeng Liu e Yanbin Li: *Security and privacy in solar insecticidal lamps internet of things: Requirements and challenges*. IEEE/CAA Journal of Automatica Sinica, 11(1):58–73, 2024.

[PS19] Diamantopoulou, Vasiliki, Nikolaos Argyropoulos, Christos Kalloniatis e Stefanos Gritzalis: *Supporting the design of privacy-aware business processes via privacy process patterns*. Em *2017 11th International Conference on Research Challenges in Information Science (RCIS)*, páginas 187–198. IEEE, 2017.

[PS20] Peixoto, Mariana Maia, Carla Silva, Helton Maia e Joao Araújo: *Towards a catalog of privacy related concepts.* Em *REFSQ Workshops*, 2020.

[PS21] Savola, Reijo M: *Towards a risk-driven methodology for privacy metrics development.* Em *2010 IEEE Second International Conference on Social Computing*, páginas 1086–1092. IEEE, 2010.

[PS22] Ferrão, Sâmmara Éllen Renner, Geovana Ramos Sousa Silva, Edna Dias Canedo e Fabiana Freitas Mendes: *Towards a taxonomy of privacy requirements based on the lgpd and iso/iec 29100.* Information and Software Technology, página 107396, 2024.

[PS23] Alkubaisy, Duaa, Karl Cox e Haralambos Mouratidis: *Towards detecting and mitigating conflicts for privacy and security requirements.* Em *2019 13th International Conference on Research Challenges in Information Science (RCIS)*, páginas 1–6. IEEE, 2019.

[PS24] Ferraris, Davide e M. Carmen Fernández Gago: *Trustapis: a trust requirements elicitation method for iot.* Int. J. Inf. Sec., 19(1):111–127, 2020. https://doi.org/10.1007/s10207-019-00438-x.

[PS25] Alves, Carina e Moisés Neves: *Especificação de requisitos de privacidade em conformidade com a lgpd: Resultados de um estudo de caso.* Em *WER*, 2021.

[PS26] Ferrao, Sâmmara Éllen Renner e Edna Dias Canedo: *Uma taxonomia para requisitos de privacidade e sua aplicação no open banking brasil.* Em *WER*, 2022.

[PS27] Gramajo, María Guadalupe, Luciana C Ballejos e Mariel Ale: *Hacia la evaluación automática de la calidad de los requerimientos de software usando redes neuronales long short term memory.* Em *WER*, 2020.

[PS28] Herwanto, Guntur Budi, Fajar J Ekaputra, Gerald Quirchmayr e A Min Tjoa: *Towards a holistic privacy requirements engineering process: Insights from a systematic literature review.* IEEE Access, 2024.

[PS29] Silva, Keyla e Laura Sarkis: *Análise de conformidade da lgpd nas instituições públicas de ensino superior no brasil sob a perspectiva dos profissionais de tic.* Em *WER*, 2023.

[PS30] Sá Sousa, Henrique Prado de, Eduardo Kinder Almentero, Tadeu Moreira de Classe, Rodrigo Juliao dos Santos e Julio César Sampaio P Leite: *Uma abordagem baseada no catálogo de requisitos não funcionais para conformidade à lgpd.* Em *WER*, 2023.

[PS31] Peixoto, Mariana, Tony Gorschek, Daniel Mendez, Davide Fucci e Carla Silva: *A natural language-based method to specify privacy requirements: an evaluation with practitioners.* Requirements Engineering, páginas 1–23, 2024.

[PS32] Alkubaisy, Duaa, Luca Piras, Mohammed Ghazi Al-Obeidallah, Karl Cox e Haralambos Mouratidis: *A framework for privacy and security requirements analysis and conflict resolution for supporting gdpr compliance through privacy-by-design.* Em *International Conference on Evaluation of Novel Approaches to Software Engineering*, páginas 67–87. Springer, 2021.

[PS33] Herwanto, Guntur Budi, Gerald Quirchmayr e A Min Tjoa: *From user stories to data flow diagrams for privacy awareness: A research preview.* Em *International Working Conference on Requirements Engineering: Foundation for Software Quality*, páginas 148–155. Springer, 2022.

[PS34] Piras, Luca, Federico Calabrese e Paolo Giorgini: *Applying acceptance requirements to requirements modeling tools via gamification: a case study on privacy and security.* Em *The Practice of Enterprise Modeling: 13th IFIP Working Conference, PoEM 2020, Riga, Latvia, November 25–27, 2020, Proceedings 13*, páginas 366–376. Springer, 2020.

[PS35] Canedo, Edna Dias, Angélica Toffano Seidel Calazans, Anderson Jefferson Cerqueira, Pedro Henrique Teixeira Costa e Eloisa Toffano Seidel Masson: *Using the design thinking empathy phase as a facilitator in privacy requirements elicitation.* Em Anderson, Bonnie Brinton, Jason Thatcher, Rayman D. Meservy, Kathy Chudoba, Kelly J. Fadel e Sue Brown (editores): *26th Americas Conference on Information Systems, AMCIS 2020, Virtual Conference, August 15-17, 2020*. Association for Information Systems, 2020. https://aisel.aisnet.org/amcis2020/info_security_privacy/info_security_privacy/27.

[PS36] Diamantopoulou, V, A Androutsopoulou, S Gritzalis e Y Charalabidis: *Preserving digital privacy in e-participation environments: Towards gdpr compliance. information, 11 (2), 117*, 2020.

[PS37] Ebrahimi, Fahimeh, Miroslav Tushev e Anas Mahmoud: *Mobile app privacy in software engineering research: A systematic mapping study.* Information and Software Technology, 133:106466, 2021.

[PS38] Omitola, Tope, Niko Tsakalakis, Gary Wills, Richard Gomer, Ben Waterson, Tom Cherret e Sophie Stalla-Bourdillon: *User configurable privacy requirements elicitation in cyber-physical systems.* Em *Adjunct Proceedings of the 30th ACM Conference on User Modeling, Adaptation and Personalization*, páginas 109–119, 2022.

[PS39] Amaral, Orlando, Sallam Abualhaija e Lionel Briand: *Ml-based compliance verification of data processing agreements against gdpr.* Em *2023 IEEE 31st international requirements engineering conference (RE)*, páginas 53–64. IEEE, 2023.

[PS40] Makri, Eleni Laskarina, Zafeiroula Georgiopoulou e Costas Lambrinoudakis: *Utilizing a privacy impact assessment method using metrics in the healthcare sector.* Information & Computer Security, 28(4):503–529, 2020.

[PS41] He, Yangyang, Paritosh Bahirat, Bart P. Knijnenburg e Abhilash Menon: *A data-driven approach to designing for privacy in household iot.* ACM Trans. Interact.

Intell. Syst., 10(1), setembro 2019, ISSN 2160-6455. https://doi.org/10.1145/3241378.

[PS42] Beckers, Kristian e Maritta Heisel: *A foundation for requirements analysis of privacy preserving software*. Em Quirchmayr, Gerald, Josef Basl, Ilsun You, Lida Xu e Edgar Weippl (editores): *Multidisciplinary Research and Practice for Information Systems*, páginas 93–107, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg, ISBN 978-3-642-32498-7.

[PS43] Deng, Mina, Kim Wuyts, Riccardo Scandariato, Bart Preneel e Wouter Joosen: *A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements*. Requirements Engineering, 16(1):3–32, 2011.

[PS44] Manna, Asmita, Anirban Sengupta e Chandan Mazumdar: *A risk-based methodology for privacy requirements elicitation and control selection*. SECURITY AND PRIVACY, 5(1):e188, 2022. https://onlinelibrary.wiley.com/doi/abs/10.1002/spy2.188.

[PS45] Argyropoulos, Nikolaos, Shaun Shei, Christos Kalloniatis, Haralambos Mouratidis, Aidan J. Delaney, Andrew Fish e Stefanos Gritzalis: *A semi-automatic approach for eliciting cloud security and privacy requirements*. Em Bui, Tung (editor): *50th Hawaii International Conference on System Sciences, HICSS 2017, Hilton Waikoloa Village, Hawaii, USA, January 4-7, 2017*, páginas 1–10. ScholarSpace / AIS Electronic Library (AISeL), 2017. https://hdl.handle.net/10125/41749.

[PS46] Hung, Patrick C. K., Marcelo Fantinato e Laura Rafferty: *A study of privacy requirements for smart toys*. Em Liang, Ting-Peng, Shin-Yuan Hung, Patrick Y. K. Chau e She-I Chang (editores): *20th Pacific Asia Conference on Information Systems, PACIS 2016, Chiayi, Taiwan, June 27 - July 1, 2016*, página 71, 2016. http://aisel.aisnet.org/pacis2016/71.

[PS47] Mouratidis, Haralambos, Christos Kalloniatis, Shareeful Islam, Marc Philippe Huget e Stefanos Gritzalis: *Aligning security and privacy to support the development of secure information systems*. J. Univers. Comput. Sci., 18(12):1608–1627, 2012.

[PS48] Sangaroonsilp, Pattaraporn, Morakot Choetkiertikul, Hoa Khanh Dam e Aditya Ghose: *An empirical study of automated privacy requirements classification in issue reports*. Automated Software Engineering, 30(2):20, 2023.

[PS49] Huth, Dominik e Florian Matthes: *"appropriate technical and organizational measures": Identifying privacy engineering approaches to meet GDPR requirements*. Em *25th Americas Conference on Information Systems, AMCIS 2019, Cancún, Mexico, August 15-17, 2019*. Association for Information Systems, 2019. https://aisel.aisnet.org/amcis2019/info_security_privacy/info_security_privacy/5.

[PS50] Beckers, Kristian: *Comparing privacy requirements engineering approaches*. Em *2012 Seventh International Conference on Availability, Reliability and Security*, páginas 574–581. IEEE, 2012.

[PS51] Alkubaisy, Duaa, Luca Piras, Mohammed Ghazi Al-Obeidallah, Karl Cox e Haralambos Mouratidis: *Confis: a tool for privacy and security analysis and conflict resolution for supporting gdpr compliance through privacy-by-design*. Em *International Conference on Evaluation of Novel Approaches to Software Engineering, ENASE-Proceedings*, volume 2021, páginas 80–91. SCITEPRESS-Science and Technology Publications, 2021.

[PS52] Ganji, Daniel, Haralambos Mouratidis, Saeed Malekshahi Gheytassi e Miltos Petridis: *Conflicts between security and privacy measures in software requirements engineering*. Em *Global Security, Safety and Sustainability: Tomorrow's Challenges of Cyber Security: 10th International Conference, ICGS3 2015, London, UK, September 15-17, 2015. Proceedings 10*, páginas 323–334. Springer, 2015.

[PS53] Gharib, Mohamad, John Mylopoulos e Paolo Giorgini: *Copri-a core ontology for privacy requirements engineering*. Em *Research Challenges in Information Science: 14th International Conference, RCIS 2020, Limassol, Cyprus, September 23–25, 2020, Proceedings 14*, páginas 472–489. Springer, 2020.

[PS54] Gharib, Mohamad, Paolo Giorgini e John Mylopoulos: *Copri v. 2—a core ontology for privacy requirements*. Data & Knowledge Engineering, 133:101888, 2021.

[PS55] Freund, Gislaine Parra, Douglas Dyllon Jeronimo de Macedo e Priscila Basto Fagundes: *Data protection and privacy: a model for evidence management*. Em Questão, 29:e–128009, 2023.

[PS56] Perera, Charith, Mahmoud Barhamgi, Arosha K Bandara, Muhammad Ajmal, Blaine Price e Bashar Nuseibeh: *Designing privacy-aware internet of things applications*. Information Sciences, 512:238–257, 2020.

[PS57] Casillo, Francesco, Vincenzo Deufemia e Carmine Gravino: *Detecting privacy requirements from user stories with nlp transfer learning models*. Information and Software Technology, 146:106853, 2022.

[PS58] Breaux, Travis D, Hanan Hibshi e Ashwini Rao: *Eddy, a formal language for specifying and analyzing data flow specifications for conflicting privacy requirements*. Requirements Engineering, 19:281–307, 2014.

[PS59] Stach, Christoph e Bernhard Mitschang: *Elicitation of privacy requirements for the internet of things using accessors*. Em *Information Systems Security and Privacy: 4th International Conference, ICISSP 2018, Funchal-Madeira, Portugal, January 22-24, 2018, Revised Selected Papers 4*, páginas 40–65. Springer, 2019.

[PS60] Martin, Yod Samuel, Jose M Del Alamo e Juan C Yelmo: *Engineering privacy requirements valuable lessons from another realm*. Em *2014 IEEE 1st International Workshop on Evolving Security and Privacy Requirements Engineering (ESPRE)*, páginas 19–24. IEEE, 2014.

[PS61] Kalloniatis, Christos, Haralambos Mouratidis e Shareeful Islam: *Evaluating cloud deployment scenarios based on security and privacy requirements*. Requirements Engineering, 18:299–319, 2013.

[PS62] Diamantopoulou, Vasiliki, Michalis Pavlidis e Haralambos Mouratidis: *Evaluation of a security and privacy requirements methodology using the physics of notation*. Em *Computer Security: ESORICS 2017 International Workshops, CyberICPS 2017 and SECPRE 2017, Oslo, Norway, September 14-15, 2017, Revised Selected Papers 3*, páginas 210–225. Springer, 2018.

[PS63] Zimmermann, Christian: *Framework and requirements for reconciling digital services and privacy*. Em *24th European Conference on Information Systems, ECIS 2016, Istanbul, Turkey, June 12-15, 2016*, página Research Paper 31, 2016. http://aisel.aisnet.org/ecis2016_rp/31.

[PS64] Schlehahn, Eva e Rigo Wenning: *GDPR transparency requirements and data privacy vocabularies*. Em Kosta, Eleni, Jo Pierson, Daniel Slamanig, Simone Fischer-Hübner e Stephan Krenn (editores): *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 de *IFIP Advances in Information and Communication Technology*, páginas 95–113. Springer, 2018. https://doi.org/10.1007/978-3-030-16744-8_7.

[PS65] Silva, Mônica da, José Viterbo, Flavia Bernardini e Cristiano Maciel: *Identifying privacy functional requirements for crowdsourcing applications in smart cities*. Em *2018 IEEE International Conference on Intelligence and Security Informatics (ISI)*, páginas 106–111, 2018.

[PS66] Mead, Nancy R, Seiya Miyazaki e Justin Zhan: *Integrating privacy requirements considerations into a security requirements engineering method and tool*. International Journal of Information Privacy, Security and Integrity, 1(1):106–126, 2011.

[PS67] Ansari, Md Tarique Jamal, Abdullah Baz, Hosam Alhakami, Wajdi Alhakami, Rajeev Kumar e Raees Ahmad Khan: *P-store: Extension of store methodology to elicit privacy requirements*. Arabian Journal for Science and Engineering, 46:8287–8310, 2021.

[PS68] Thapa, Chandra e Seyit Camtepe: *Precision health data: Requirements, challenges and existing techniques for data security and privacy*. Computers in biology and medicine, 129:104130, 2021.

[PS69] Radics, Peter J, Denis Gracanin e Dennis Kafura: *Preprocess before you build: Introducing a framework for privacy requirements engineering*. Em *2013 International Conference on Social Computing*, páginas 564–569. IEEE, 2013.

[PS70] Rösch, Daniel, Thomas Schuster, Lukas Waidelich e Sascha Alpers: *Privacy control patterns for compliant application of GDPR*. Em *25th Americas Conference*

on Information Systems, AMCIS 2019, Cancún, Mexico, August 15-17, 2019. Association for Information Systems, 2019. https://aisel.aisnet.org/amcis2019/info_security_privacy/info_security_privacy/27.

[PS71] Anthonysamy, Pauline, Awais Rashid e Ruzanna Chitchyan: *Privacy requirements: present & future*. Em *2017 IEEE/ACM 39th international conference on software engineering: software engineering in society track (ICSE-SEIS)*, páginas 13–22. IEEE, 2017.

[PS72] Tsohou, Aggeliki, Emmanouil Magkos, Haralambos Mouratidis, George Chrysoloras, Luca Piras, Michalis Pavlidis, Julien Debussche, Marco Rotoloni e Beatriz Gallego-Nicasio Crespo: *Privacy, security, legal and technology acceptance elicited and consolidated requirements for a gdpr compliance platform*. Information & Computer Security, 28(4):531–553, 2020.

[PS73] Gjermundrød, Harald, Ioanna Dionysiou e Kyriakos Costa: *privacytracker: a privacy-by-design gdpr-compliant framework with verifiable data traceability controls*. Em *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*, páginas 3–15. Springer, 2016.

[PS74] Mouratidis, Haralambos e Paolo Giorgini: *Secure tropos: a security-oriented extension of the tropos methodology*. International Journal of Software Engineering and Knowledge Engineering, 17(02):285–309, 2007.

[PS75] Pattakou, Argyri, Christos Kalloniatis e Stefanos Gritzalis: *Security and privacy requirements engineering methods for traditional and cloud-based systems: a review*. Cloud Comput, 2017:155, 2017.

[PS76] Kang, Giluk, Jahoon Koo e Young Gab Kim: *Security and privacy requirements for the metaverse: A metaverse applications perspective*. IEEE Communications Magazine, 62(1):148–154, 2023.

[PS77] Jensen, Carlos, Joe Tullio, Colin Potts e Elizabeth D Mynatt: *Strap: a structured analysis framework for privacy*. Georgia Institute of Technology, 1, 2005.

[PS78] Ayala-Rivera, Vanessa e Liliana Pasquale: *The grace period has ended: An approach to operationalize gdpr requirements*. Em *2018 IEEE 26th International Requirements Engineering Conference (RE)*, páginas 136–146. IEEE, 2018.

[PS79] Pattakou, Argyri, Aikaterini Georgia Mavroeidi, Vasiliki Diamantopoulou, Christos Kalloniatis e Stefanos Gritzalis: *Towards the design of usable privacy by design methodologies*. Em *2018 IEEE 5th International Workshop on Evolving Security & Privacy Requirements Engineering (ESPRE)*, páginas 1–8. IEEE, 2018.

[PS80] Sheth, Swapneel, Gail Kaiser e Walid Maalej: *Us and them: a study of privacy requirements across north america, asia, and europe*. Em *Proceedings of the 36th International Conference on Software Engineering*, páginas 859–870, 2014.

[PS81] Kalloniatis, Christos, Evangelia Kavakli e Stefanos Gritzalis: *Using privacy process patterns for incorporating privacy requirements into the system design process.* Em *The Second International Conference on Availability, Reliability and Security (ARES'07)*, páginas 1009–1017. IEEE, 2007.

[PS82] Gopi, Geetika, Aadyaa Maddi, Omkhar Arasaratnam e Giulia Fanti: *Privacy requirements and realities of digital public goods.* Em *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)*, páginas 159–177, 2024.

[PS83] Melo, Ruy Ovídio Perrelli de, Jéssyka Vilela e Carla Silva: *Do entendimento à aplicação: Requisitos de privacidade e a visão dos usuários sobre a LGPD.* Em Lucena, Márcia, Maria Lencastre e Luciana C. Ballejos (editores): *Anais do WER24 - Workshop em Engenharia de Requisitos, Buenos Aires, Argentina, August 7-9, 2024*. Even3, Brasil, 2024. https://doi.org/10.29327/1407529.27-27.

[PS84] Vieira, Arthur, Mariana Maia Peixoto e Carla Silva: *Um modelo de conceitos relacionados à privacidade de dados pessoais.* Em Antonelli, Leandro, Márcia Lucena e Roxana L. Q. Portugal (editores): *Anais do WER23 - Workshop em Engenharia de Requisitos, Porto Alegre, RS, Brasil, August 15-17, 2023*. LFS (UFRN, Brasil), 2023. https://doi.org/10.29327/1298356.26-6.

[PS85] Santana, Egberto, Jéssyka Vilela e Mariana Maia Peixoto: *Diretrizes para apresentação de políticas de privacidade voltadas à experiência do usuário.* Em *WER*, 2022.

[PS86] Valença, George, Maria Wanick Sarinho, Vinícius Polito e Fernando Lins: *Do platforms care about your child's data? a proposal of legal requirements for children's privacy and protection.* Em *WER*, 2022.

[PS87] Terra, Augusto H, Jéssyka Vilela e Mariana Maia Peixoto: *A catalog of quality criteria to guide the assessment of applications' privacy policies.* Em *WER*, 2022.

[PS88] Santos, Sarah, Sara Haghighi, Sepideh Ghanavati, Travis D Breaux e Thomas B Norton: *Patterns of inquiry in a community forum for legal compliance with privacy law.* Em *2024 IEEE 32nd International Requirements Engineering Conference Workshops (REW)*, páginas 251–259. IEEE, 2024.

[PS89] Benthall, Sebastian e Rachel Cummings: *Integrating differential privacy and contextual integrity.* Em *Proceedings of the Symposium on Computer Science and Law*, páginas 9–15, 2024.

[PS90] Shah, Tejas e Parul Patel: *Design of a privacy taxonomy in requirement engineering.* Em *International Conference on IoT Based Control Networks and Intelligent Systems*, páginas 703–716. Springer, 2023.

[PS91] Belhajjame, Khalid, Noura Faci, Zakaria Maamar, Vanilson Burégio, Edvan Soares e Mahmoud Barhamgi: *On privacy-aware escience workflows.* Computing, 102:1171–1185, 2020.

[PS92] Kanwal, Tehsin, Adeel Anjum e Abid Khan: *Privacy preservation in e-health cloud: taxonomy, privacy requirements, feasibility analysis, and opportunities.* Cluster Computing, 24(1):293–317, 2021.

[PS93] Campanile, Lelio, Mauro Iacono e Michele Mastroianni: *Towards privacy-aware software design in small and medium enterprises.* Em *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 Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)*, páginas 1–8. IEEE, 2022.

[PS94] Mashaly, Bahgat, Sahar Selim, Ahmed H Yousef e Khaled M Fouad: *Privacy by design: A microservices-based software architecture approach.* Em *2022 2nd International Mobile, Intelligent, and Ubiquitous Computing Conference (MIUCC)*, páginas 357–364. IEEE, 2022.

[PS95] Rafiei, Majid e Wil MP van der Aalst: *Privacy-preserving continuous event data publishing.* Em *Business Process Management Forum: BPM Forum 2021, Rome, Italy, September 06–10, 2021, Proceedings 19*, páginas 178–194. Springer, 2021.

[PS96] Herwanto, Guntur Budi, Diyah Utami Kusumaning Putri, Annisa Maulida Ningtyas, Anis Fuad, Gerald Quirchmayr e A Min Tjoa: *Integrating contextual integrity in privacy requirements engineering: A study case in personal e-health applications.* Em *International Conference on Innovations for Community Services*, páginas 237–256. Springer, 2024.

[PS97] Liang, Wenjuan, Hong Chen, Ruixuan Liu, Yuncheng Wu e Cuiping Li: *A pufferfish privacy mechanism for monitoring web browsing behavior under temporal correlations.* Computers & Security, 92:101754, 2020.

[PS98] Herwanto, Guntur Budi, Gerald Quirchmayr e A. Min Tjoa: *Learning to rank privacy design patterns: A semantic approach to meeting privacy requirements.* Em Mendez, Daniel e Ana Moreira (editores): *Requirements Engineering: Foundation for Software Quality*, páginas 57–73, Cham, 2024. Springer Nature Switzerland, ISBN 978-3-031-57327-9.

[PS99] Anish, Preethu Rose, Aparna Verma, Sivanthy Venkatesan, Logamurugan V. e Smita Ghaisas: *Governance-focused classification of security and privacy requirements from obligations in software engineering contracts.* Em Mendez, Daniel e Ana Moreira (editores): *Requirements Engineering: Foundation for Software Quality*, páginas 92–108, Cham, 2024. Springer Nature Switzerland, ISBN 978-3-031-57327-9.

[PS100] McDonald, Nora e Andrea Forte: *The politics of privacy theories: Moving from norms to vulnerabilities.* Em *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, páginas 1–14, 2020.

[PS101] Bondel, Gloria, Gonzalo Munilla Garrido, Kevin Baumer e Florian Matthes: *The use of de-identification methods for secure and privacy-enhancing big data analytics in cloud environments.* Em *ICEIS (2)*, páginas 338–344, 2020.

[PS102] Canedo, Edna Dias, Angelica Toffano Seidel Calazans, Anderson Jefferson Cerqueira, Pedro Henrique Teixeira Costa e Eloisa Toffano Seidel Masson: *Agile teams' perception in privacy requirements elicitation: Lgpd's compliance in brazil*. Em *2021 IEEE 29th International Requirements Engineering Conference (RE)*, páginas 58–69. IEEE, 2021.

[PS103] Mouratidis, Haralambos, Shaun Shei e Aidan Delaney: *A security requirements modelling language for cloud computing environments*. Software and Systems Modeling, 19(2):271–295, 2020.

[PS104] Bijwe, Ashwini e Nancy R Mead: *Adapting the square process for privacy requirements engineering*. Software Engineering Institute: Pittsburgh, PA, USA, 2010.

[PS105] Olukoya, Oluwafemi: *Assessing frameworks for eliciting privacy & security requirements from laws and regulations*. Computers & Security, 117:102697, 2022.

[PS106] Roberts, Joshua D, Joanna F DeFranco e D Richard Kuhn: *Data block matrix and hyperledger implementation: extending distributed ledger technology for privacy requirements*. Distributed Ledger Technologies: Research and Practice, 2(2):1–11, 2023.

[PS107] Veseli, Fatbardh, Jetzabel Serna Olvera, Tobias Pulls e Kai Rannenberg: *Engineering privacy by design: lessons from the design and implementation of an identity wallet platform*. Em *Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing*, páginas 1475–1483, 2019.

[PS108] Kavakli, Evangelia, Christos Kalloniatis, Pericles Loucopoulos e Stefanos Gritzalis: *Incorporating privacy requirements into the system design process: the pris conceptual framework*. Internet research, 16(2):140–158, 2006.

[PS109] Mai, Phu X, Arda Goknil, Lwin Khin Shar, Fabrizio Pastore, Lionel C Briand e Shaban Shaame: *Modeling security and privacy requirements: a use case-driven approach*. Information and Software Technology, 100:165–182, 2018.

[PS110] Dias Canedo, Edna, Angelica Toffano Seidel Calazans, Eloisa Toffano Seidel Masson, Pedro Henrique Teixeira Costa e Fernanda Lima: *Perceptions of ict practitioners regarding software privacy*. Entropy, 22(4):429, 2020.

[PS111] Gharib, Mohamad, Mattia Salnitri, Elda Paja, Paolo Giorgini, Haralambos Mouratidis, Michalis Pavlidis, José F Ruiz, Sandra Fernandez e Andrea Della Siria: *Privacy requirements: findings and lessons learned in developing a privacy platform*. Em *2016 IEEE 24th International Requirements Engineering Conference (RE)*, páginas 256–265. IEEE, 2016.

[PS112] Ahmadian, Amir Shayan, Daniel Strüber e Jan Jürjens: *Privacy-enhanced system design modeling based on privacy features*. Em *Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing*, páginas 1492–1499, 2019.

[PS113] Peixoto, Mariana Maia e Carla Silva: *Specifying privacy requirements with goal-oriented modeling languages.* Em *Proceedings of the XXXII Brazilian symposium on software engineering*, páginas 112–121, 2018.

[PS114] Coles, Joshua, Shamal Faily e Duncan Ki-Aries: *Tool-supporting data protection impact assessments with cairis.* Em *2018 IEEE 5th International Workshop on Evolving Security & Privacy Requirements Engineering (ESPRE)*, páginas 21–27. IEEE, 2018.

[PS115] Islam, Shareeful, Haralambos Mouratidis e Stefan Wagner: *Towards a framework to elicit and manage security and privacy requirements from laws and regulations.* Em *Requirements Engineering: Foundation for Software Quality: 16th International Working Conference, REFSQ 2010, Essen, Germany, June 30–July 2, 2010. Proceedings 16*, páginas 255–261. Springer, 2010.

[PS116] Gharib, Mohamad, Paolo Giorgini e John Mylopoulos: *Towards an ontology for privacy requirements via a systematic literature review.* Em *Conceptual Modeling: 36th International Conference, ER 2017, Valencia, Spain, November 6–9, 2017, Proceedings 36*, páginas 193–208. Springer, 2017.

[PS117] Jesus, Ewerton David Brito de, Jéssyka Vilela e Carla Silva: *Requisitos de segurança e privacidade em startups: Um estudo empírico em uma aplicação de governança de dados.* Em Lucena, Márcia, Maria Lencastre e Luciana C. Ballejos (editores): *Anais do WER24 - Workshop em Engenharia de Requisitos, Buenos Aires, Argentina, August 7-9, 2024*. Even3, Brasil, 2024. https://doi.org/10.29327/1407529.27-13.

[PS118] Bondel, Gloria, Gonzalo Munilla Garrido, Kevin Baumer e Florian Matthes: *Towards a privacy-enhancing tool based on de- identification methods.* Em Vogel, Doug, Kathy Ning Shen, Pan Shan Ling, Carol Hsu, James Y. L. Thong, Marco De Marco, Moez Limayem e Sean Xin Xu (editores): *24th Pacific Asia Conference on Information Systems, PACIS 2020, Dubai, UAE, June 22-24, 2020*, página 157, 2020. https://aisel.aisnet.org/pacis2020/157.

[PS119] Zinsmaier, Sandra Domenique, Hanno Langweg e Marcel Waldvogel: *A practical approach to stakeholder-driven determination of security requirements based on the gdpr and common criteria.* Em *ICISSP*, páginas 473–480, 2020.

[PS120] Anwar, Memoona J e Asif Gill: *Developing an integrated iso 27701 and gdpr based information privacy compliance requirements model.* Em *Australasian Conference on Information Systems 2020*, 2021.

[PS121] Huang, Tianjian, Vaishnavi Kaulagi, Mitra Bokaei Hosseini e Travis Breaux: *Mobile application privacy risk assessments from user-authored scenarios.* Em *2023 IEEE 31st International Requirements Engineering Conference (RE)*, páginas 17–28. IEEE, 2023.

[PS122] Sindre, Guttorm e Andreas L Opdahl: *Eliciting security requirements with misuse cases.* Requirements engineering, 10:34–44, 2005.

[PS123] Krishnan, Padmanabhan e Kostyantyn Vorobyov: *Enforcement of privacy requirements*. Computers & Security, 52:164–177, 2015.

[PS124] Kalloniatis, Christos, Evangelia Kavakli e Efstathios Kontellis: *Pris tool: A case tool for privacy-oriented requirements engineering*. Em Poulymenakou, Angeliki, Nancy Pouloudi e Katerina Pramatari (editores): *The 4th Mediterranean Conference on Information Systems, MCIS 2009, Athens University of Economics and Business, AUEB, Athens, Greece, 25-27 September 2009*, página 71. Athens University of Economics and Business / AISeL, 2009. http://aisel.aisnet.org/mcis2009/71.

[PS125] Pullonen, Pille, Jake Tom, Raimundas Matulevičius e Aivo Toots: *Privacy-enhanced bpmn: enabling data privacy analysis in business processes models*. Software and Systems Modeling, 18:3235–3264, 2019.

Apêndice A

Selected Papers

Tabela A.1: Estudos selecionados de 2005 a 2024: Legenda: ID = Número do Estudo; T= Técnicas; M = Métodos; P = Processos; F = Frameworks; T = Ferramentas; N = Não; Y = Sim; NE = Número de Experimentos; A = Academia; I = Indústria; IL = Ilustrativo

ID	**Título/Referência**	**T/M/P/F/T**	**Framework (Y/N)**	**RQ**	**NE (A, I, IL)**
S1	Dealing with privacy issues during the system design process [PS6]	Privacy by Design, Enterprise Knowledge Development Framework	Y - PriS	1, 3, 4	0 - A
S2	Eliciting security requirements with misuse cases [PS122]	Misuse Cases, Lightweight and Extensive Descriptions, Guidelines for Working with Misuse Cases, Integration with Existing Standards, Elicitation Process, Analysis of Security Threats, Goal-Oriented Frameworks, Use-Case Driven Frameworks, Tool-Supported Methods, Security Threat Categories, Empirical Evaluation	Y	1, 3, 4	0 - IL

Tabela A.1 – Estudos selecionados de 2005 a 2024

ID	Título/Referência	T/M/P/F/T	Framework (Y/N)	RQ	NE (A, I, IL)
S3	STRAP: A Structured Analysis Framework for Privacy [PS77]	FIP, Bellotti and Sellen framework	Y - STRAP	1, 3	0 - A
S4	Incorporating privacy requirements into the system design process: The PriS conceptual framework [PS108]	PriS Methodology, Evaluation Procedure, Enterprise Knowledge Development (EKD) Framework, Case Tools Development, Ontology Development	Y - PriS	1, 3, 4	0 - I
S5	Protecting privacy in system design: The electronic voting case [PS15]	Non-Functional Requirements, Tropos, KAOS, i* , Role-Based Access Control, GBRAM, M-N framework, Bellotti and Sellen's framework, STRAP, PriS, Identity management tools, Biometrics, Smart Cards, Permission Management and Monitoring tools	Y	1, 4	0 - A
S6	Secure Tropos: A Security-Oriented Extension of the Tropos Methodology [PS74]	Modeling techniques, Tropos methodology, Tropos process, PKI/trust management requirements specification and analysis framework	Y - Secure Tropos	1, 3, 4	5 - A
S7	Using Privacy Process Patterns for Incorporating Privacy Requirements into the System Design Process [PS81]	PriS Framework	Y	1, 3	0 - A

Tabela A.1 – Estudos selecionados de 2005 a 2024

ID	Título/Referência	T/M/P/F/T	Framework (Y/N)	RQ	NE (A, I, IL)
S8	Addressing privacy requirements in system design: the PriS method [PS2]	Privacy-Enhancing Technologies and elicitation, PriS Method and goal oriented analisis, Privacy Goal Elicitation, Implementation Process, STRAP Framework, Automated Tools	Y - PriS Method	1, 3, 4	0 - A

Tabela A.1 – Estudos selecionados de 2005 a 2024

ID	Título/Referência	T/M/P/F/T	Framework (Y/N)	RQ	NE (A, I, IL)
S9	Computer-Aided Privacy Requirements Elicitation Technique [PS5]	Misuse Cases, Soft Systems Methodology, Quality Function Deployment, Controlled Requirements Expression, Issue-based information systems, join application development, feature-oriented domain analysis, critical discourse analysis, accelerated requirements method, SQUARE, OECD Privacy Statement Generator, OECD Guidelines on the Protection of Privacy, The European Commission's Directive on Data Protection, Japanese Act on the Protection of Personal Information, The Health Insurance Portability and Accountability Act, The Family Educational Rights and Privacy Act, CA_SB_1386 (California), Video Privacy Protection Act, The Privacy Protection Act, The Children's Online Privacy Protection Act, Common Criteria, W3C Web Services Architecture Requirements	Y	1, 4	0 - I

Tabela A.1 – Estudos selecionados de 2005 a 2024

ID	Título/Referência	T/M/P/F/T	Framework (Y/N)	RQ	NE (A, I, IL)
S10	Engineering Privacy [PS8]	k-anonymity, Privacy by policy, privacy by architecture, privacy requirements analysis, system design framework	N	1, 3, 4	0 - I
S11	Pris Tool: A Case Tool For Privacy Oriented Requirements Engineering [PS124]	Implementation Techniques, Correlation Analysis, PriS Methodology, Privacy Requirements Elicitation, Monitoring and Impact Assessment, PriS Conceptual Framework, User Interface Features	Y - PriS Tool	1, 3, 4	0 - IL
S12	Adapting the square process for Privacy Requirements Engineering [PS104]	Structured or unstructured interviews, use and misuse cases, goal-based requirements analysis method, pattern based approach, Pair-Wise Comparison Method, A Method for Prioritization of Legal Requirements, SQUARE process, Privacy Requirements Elicitation Technique (PRET)	N	1, 3	0 - I

Tabela A.1 – Estudos selecionados de 2005 a 2024

ID	Título/Referência	T/M/P/F/T	Framework (Y/N)	RQ	NE (A, I, IL)
S13	Towards a framework to elicit and manage security and privacy requirements from laws and regulations [PS115]	Goal-driven risk management (GSRM) Security Attack Scenarios (SAS), Secure Tropos methodology, Elicitation and management of security and privacy requirements, Secure Tropos modelling language, User Requirement Notation based on Goal-oriented Requirement Language	Y	1, 3, 4	0 - I
S14	Towards a Risk-Driven Methodology for Privacy Metrics Development [PS21]	Identification of Basic Measurable Component, Information Technology Security Evaluation Criteria (ITSEC), Cloud Security Alliance (CSA), EuroPriSe	Y	1, 3, 4	0 - A
S15	A privacy threat analysis framework: Supporting the elicitation and fulfillment of privacy requirements [PS43]	Privacy threat modeling techniques, framework that uses i* to deal with security and privacy requirements, Administrative tools, Information tools, Anonymizer products, services, and architectures, Pseudonymizer tools, Track and evidence erasers,	Y	1, 3, 4	0 - A

Tabela A.1 – Estudos selecionados de 2005 a 2024

ID	Título/Referência	T/M/P/F/T	Framework (Y/N)	RQ	NE (A, I, IL)
S16	Integrating privacy requirements considerations into a security requirements engineering method and tool [PS66]	Misuse cases, Soft systems methodology, Quality function deployment, Controlled requirements expression, Issue-based information systems, Joint application development, Feature-oriented domain analysis, Critical discourse analysis, Accelerated requirements method , SQUARE, PriS	Y - PRET	1, 3, 4	0 - A
S17	A foundation for requirements analysis of privacy preserving software [PS42]	Anonymity, pseudonymity, unlinkability, and unobservability, method for privacy requirements elicitation using privacy patterns, privacy threat analysis framework	Y	4	0 - A

Tabela A.1 – Estudos selecionados de 2005 a 2024

ID	Título/Referência	T/M/P/F/T	Framework (Y/N)	RQ	NE (A, I, IL)
S18	Aligning Security and Privacy to Support the Development of Secure Information Systems [PS47]	Onion routing, Identity management, Anonymity Process Pattern, Anonymity, i* method, Tropos method, KAOS method, GBRAM (Goal-Based Requirements Analysis Method), RBAC (Role-Based Access Control), STRAP (STRuctured Analysis for Privacy), Anonymity Process Pattern, Integrity Process Pattern, Summarizing Response Process Pattern, NFR (Non-Functional Requirement Framework), M-N (Moffett-Nuseibeh Framework), B-S (Bellotti-Sellen Framework), PriS (Privacy Safeguard)	Y	1, 3, 4	0 - A
S19	Applying Soft Computing Technologies for Implementing Privacy-Aware Systems [PS3]	Pris Method, identification and analysis of the impact of privacy goals on organizational processes, the modeling of privacy-related processes based on relevant privacy process patterns, and the definition of the system architecture that supports these processes, Enterprise Knowledge Development	Y	1, 3, 4	0 - A

Tabela A.1 – Estudos selecionados de 2005 a 2024

ID	Título/Referência	T/M/P/F/T	Framework (Y/N)	RQ	NE (A, I, IL)
S20	Comparing Privacy Requirements Engineering Approaches [PS50]	PriS, LINDDUN, Framework for Privacy-Friendly System Design	Y	1, 3, 4	0 - A
S21	Enforcement of privacy requirements [PS123]	Dynamic role-based access control (RBAC), Formal verification of role-based access control policies Policy authoring and enforcement mechanisms, Development of privacy policies from requirements, Enforcement of privacy requirements through automata	Y	1, 3, 4	0 - IL
S22	Evaluating cloud deployment scenarios based on security and privacy requirements [PS61]	Modeling languages, Secure Tropos, PriS, organizational analysis, security and privacy requirements analysis, and selection of deployment model	Y	1, 3, 4	0 - A
S23	Preprocess before You Build: Introducing a Framework for Privacy Requirements Engineering [PS69]	PREprocess Framework	Y - PREprocess	4	0 - A

Tabela A.1 – Estudos selecionados de 2005 a 2024

ID	Título/Referência	T/M/P/F/T	Framework (Y/N)	RQ	NE (A, I, IL)
S24	Eddy, a formal language for specifying and analyzing data flow specifications for conflicting privacy requirements [PS58]	Mapping privacy-related policies to a formalization using verb heuristics, conflict detection through description logic (DL) subsumption, case study research method, exploratory case studies of privacy policies from platforms, Eddy language, TAMS Analyzer	Y - Eddy language	1, 3, 4	0 - A
S25	Engineering privacy requirements valuable lessons from another realm [PS60]	Technology-neutral and technology-specific patterns, Privacy by Design, ISO/IEC 29100, OASIS Privacy Management Reference Model and Methodology	Y	1, 3, 4	0 - A
S26	Us and them: a study of privacy requirements across north america, asia, and europe [PS80]	Anonymization	Y	1, 3, 4	595 - A
S27	Conflicts Between Security and Privacy Measures in Software Requirements Engineering [PS52]	KAOS, Tropos, GBRAM, RBAC, i*, PbD, STRAP, PriS, NFR, M-N, B-S, Caprice	N	1, 4	0 - A
S28	Privacy by Design in Federated Identity Management [PS13]	Privacy by Design, Federated Identity Management	N	1, 3	0 - A

Tabela A.1 – Estudos selecionados de 2005 a 2024

ID	Título/Referência	T/M/P/F/T	Framework (Y/N)	RQ	NE (A, I, IL)
S29	A Study of Privacy Requirements for Smart toys [PS46]	Homomorphism Encryption, Privacy Policy Analysis, User-Centric Approaches, Elicitation, Implementation of Parental Controls, Parental Control Features, Children's Vulnerability, Legislative Context	N	1, 3, 4	0 - A
S30	Framework and Requirements for Reconciling Digital Services and Privacy [PS63]	Reconciliation Mechanisms (RMs), Signaling and Screening Mechanisms, Contract Design and Negotiation, Accountability Conceptualization, Monitoring and Compliance Detection, Data Analysis and Purpose Limitation, Accountability-Centric Framework, Reconciliation Framework,	Y	1, 3, 4	0 - A
S31	Privacy Requirements: Findings and Lessons Learned in Developing a Privacy Platform [PS111]	Questionnaire-based technique, Scenario-based technique	Y	1, 3, 4	24 - I
S32	PrivacyTracker: A Privacy-by-Design GDPR-Compliant Framework with Verifiable Data Traceability Controls [PS73]	A tree-like data structure , Data validation techniques, Windows, Apache, MySQL, PHP, GDPR Compliance, Data Disclosure Issues, Cryptographic Techniques	Y - Privacy-Tracker	1, 4	16 - A

Tabela A.1 – Estudos selecionados de 2005 a 2024

ID	Título/Referência	T/M/P/F/T	Framework (Y/N)	RQ	NE (A, I, IL)
S33	A semi-automatic approach for eliciting cloud security and privacy requirements [PS45]	Secure Tropos approach, Secure Tropos methodology, PriS framework	Y	1, 3, 4	0 - A
S34	Privacy Requirements: Present & Future [PS71]	Compliance, Access Control, Verification, Usability, Commitment Analysis, Semantic Parametrisation, Formal Methods for Verification, Automated Trace Retrievals, Ibex, HIPAA, REQMON	N	1, 4	0 - A
S35	Security and Privacy Requirements Engineering Methods for Traditional and Cloud-Based Systems: A Review [PS75]	SQUARE, MOSRE, SREP, Tropos, KAOS, PresSure, SQUARE, PriS, SREF, LINDDUN	N	1, 4	0 - A
S36	Supporting the Design of Privacy-Aware Business Processes via Privacy Process Patterns [PS19]	PriS methodology, authentication, authorisation, anonymity, pseudonymity, unlinkability, undetectability, unobservability, data protection, identity management, biometris, smart cards, permission managements, monitoring and audit tools. Browsing pseudonyms, virtual email addresses, trusted third parties, crowds, onion routing, DC-nets, Mix-nets, hordes, GAP, Tor, aggregation gateway, dynamic location granularity	Y	1, 4	0 - A

Tabela A.1 – Estudos selecionados de 2005 a 2024

ID	Título/Referência	T/M/P/F/T	Framework (Y/N)	RQ	NE (A, I, IL)
S37	Towards an Ontology for Privacy Requirements via a Systematic Literature Review [PS116]	Graphical Notation, Requirements Engineering Process, Secure Tropos Framework	N	1, 3, 4	0 - I
S38	Assurance of Security and Privacy Requirements for Cloud Deployment Models [PS4]	OMG standard Software, Systems Process Engineering Metamodel (SPEM) version 2.0	Y	1, 3	0 - I
S39	Early Privacy: Approximating Mental Models in the Definition of Privacy Requirements in Systems Design [PS7]	Questionnaires, participatory design sessions,	N	4	20 - A
S40	Evaluation of a security and privacy requirements methodology using the physics of notation [PS62]	Secure Tropos methodology, Cognitive Dimensions Framework, SecTro	N	1, 3, 4	0 - A
S41	Identifying Privacy Functional Requirements for Crowdsourcing Applications in Smart Cities [PS65]	Data encryption, Homomorphic encryption, Commitment mechanism, Secret sharing, Zero-knowledge proof, Differential privacy, Data minimization, Privacy by Design	N	1, 4	0 - A

Tabela A.1 – Estudos selecionados de 2005 a 2024

ID	Título/Referência	T/M/P/F/T	Framework (Y/N)	RQ	NE (A, I, IL)
S42	Modeling Security and Privacy Requirements: a Use Case-Driven Approach [PS109]	Risk/threat analysis-based approaches, Problem frame-based approaches, Common criteria-based approaches, Natural language processing for reporting inconsistencies, SQUARE framework, RMCM-V, Papyrus, IBM Doors	Y - RMCM	1, 3, 4	4 - I
S43	Specifying privacy requirements with goal-oriented modeling languages [PS113]	Framework of privacy modeling capabilities, NFR-Framework, Secure-Tropos	Y	1, 3, 4	8 - I
S44	The Grace Period Has Ended: An Approach to Operationalize GDPR Requirements [PS78]	Pseudonymization and Privacy by Design, Business Analysis Body of Knowledge, ISO 29100 Privacy Framework, SMART and ISO/IEC/IEEE 29148	y - GuideMe	4	40 - A
S45	Tool-Supporting Data Protection Impact Assessments with CAIRIS [PS114]	Usability techniques, Security techniques, Requirements Engineering techniques associated with IRIS, Data Protection Impact Assessment (DPIA) methods, Stakeholder interviews, IRIS meta-model, CAIRIS framework	Y	1, 4	0 - I
S46	Towards the Design of Usable Privacy by Design Methodologies [PS79]	LINDDUN, SQUARE, PriS, RBAC, STRAP, i* method, Secure Tropos with PriS, ISO 9241-11	N	1, 4	0 - A

Tabela A.1 – Estudos selecionados de 2005 a 2024

ID	Título/Referência	T/M/P/F/T	Framework (Y/N)	RQ	NE (A, I, IL)
S47	A Data-Driven Approach to Designing for Privacy in Household IoT [PS41]	User Feedback Collection, Statistical Analysis, Mediation Analysis, Post-Hoc Testing, Interface Design Process, Data Collection Process, Privacy Profiles Framework, Statistical Software, User-Centered Design, Trade-offs in Design	Y	1, 4	1133 - A
S48	Appropriate Technical and Organizational Measures Identifying Privacy Engineering Approaches to Meet GDPR Requirements [PS49]	KAOS, GBRAM, i*, Tropos, NFR, RBAC, Easy Win-Win, B-S, STRAP, PriS, LINDDUN, SCuriTas, GDPR	N	1, 4	0 - A
S49	Elicitation of Privacy Requirements for the Internet of Things Using ACCESSORS [PS59]	Modeling Techniques, Privacy Rule Definition, Elicitation, Mapping Policy Rules, Data Blocking and Filtering, Privacy Management Platform (PMP)	Y - ACCESSORS	1, 3, 4	0 - A
S50	Engineering Privacy by Design – Lessons from the Design and Implementation of an Identity Wallet Platform [PS107]	Privacy by Design, PRIPARE, LINDDUN, STRIDE	N	1, 4	0 - I
S51	GDPR Transparency Requirements and Data Privacy Vocabularies [PS64]	Technical Specifications, Semantification, Taxonomy Development, W3C Frameworks, GDPR Compliance Framework,	N	1, 3, 4	0 - A

Tabela A.1 – Estudos selecionados de 2005 a 2024

ID	Título/Referência	T/M/P/F/T	Framework (Y/N)	RQ	NE (A, I, IL)
S52	Modelling the interplay of security, privacy and trust in sociotechnical systems: a computer-aided design approach [PS11]	PRET, i* method, SQUARE, SePTA, PriS, STS-tool, SecTro	Y	1, 3, 4	0 - I
S53	PCM Tool: Privacy Requirements Specification in Agile Software Development [PS12]	Privacy Criteria Method (PCM)	Y - PCM	1, 3	34 - I
S54	Privacy Control Patterns for Compliant Application of GDPR [PS70]	Privacy by Default, GDPR	N	1, 3	0 - A
S55	Privacy-enhanced BPMN: enabling data privacy analysis in business processes models [PS125]	Business Process Model and Notation (BPMN), multi-leveled model of PET abstraction	Y - PE-BPMN	1, 3, 4	0 - IL
S56	Privacy-Enhanced System Design Modeling Based on Privacy Features [PS112]	Privacy impact assessment (PIA) methodology, Function Point Analysis (FPA), Reusable Aspect Models (RAMs),	Y	1, 3	0 - I
S57	Recommender-based Privacy Requirements Elicitation — EPICUREAN [PS16]	Suppression, obfuscation, reordering, Hierarchical modeling technique, Supervised learning approach, Natural Language Processing (NLP), RAKE algorithm, GDPR	Y - EPICUREAN	1, 3, 4	0 - I

Tabela A.1 – Estudos selecionados de 2005 a 2024

ID	Título/Referência	T/M/P/F/T	Framework (Y/N)	RQ	NE (A, I, IL)
S58	Towards Detecting and Mitigating Conflicts for Privacy and Security Requirements [PS23]	Cryptographic, Steganographic technologies, Onion routing, trusted third parties, Dummy traffic, Zero-Knowledge Proofs of Knowledge (ZKPoKs), K-anonymity, Searchable encryption, Public key	Y	4	0 - A
S59	A security requirements modelling language for cloud computing [PS103]	Cloud security analysis, Security mitigation analysis, Transparency analysis, Modelling language based on Secure Tropos, i*, PRiS, Requirements elicitation process, Secure cloud process Framework for eliciting security and privacy requirements, Apparatus Software Tool	Y	1, 3, 4	0 - I
S60	COPri - A Core Ontology for Privacy Requirements Engineering [PS53]	Scope & Objective Identification, Knowledge Acquisition, Conceptualization, Implementation, Evaluation and Validation, Ontology Development and Systematic Literature Review	Y - COPri	1, 3, 4	16 - A
S61	Designing privacy-aware internet of things applications [PS56]	Richards' three-tier coding technique, Privacy by Design framework	Y	4	16 - A

Tabela A.1 – Estudos selecionados de 2005 a 2024

ID	Título/Referência	T/M/P/F/T	Framework (Y/N)	RQ	NE (A, I, IL)
S62	Perceptions of ICT practitioners regarding software privacy [PS110]	User story, Use Cases, Interviews, Process Modeling, User Experience, Design Thinking, Design Sprint, Formal models, Focal groups, Prototyping and own process, Privacy by Design, Pris Tool, PCM Tool, Computer-Aided Privacy Requirements Elicitation Technique	N	1, 3, 4	68 - I
S63	Privacy, security, legal and technology acceptance elicited and consolidated requirements for a GDPR compliance platform [PS72]	Human-Centered Design (HCD) approach, MoSCoW classification for prioritizing requirements	N	1, 3, 4	215 - A
S64	Towards a Catalog of Privacy Related Concepts [PS20]	KAOS, i* language, Tropos, Problem Frames, SI* modeling, GRL, Threat Model, Use Case Maps, SecBPMN-ml. UML4PF, Data Flow Diagram, Goal/Agent Modeling, Secure Tropos, Misuse cases, UMLsec, UML, STS-ml, Legal GRL, CORAS Risk Modeling, User Requirements Notation, BPMN, Security-Aware Tropos, Threat Tree, NFR	N	1, 3, 4	0 - A
S65	TrUStAPIS: a trust requirements elicitation method for IoT [PS24]	Secure Tropos, K-model	Y - TrUStAPIS	1, 3	0 - I

Tabela A.1 – Estudos selecionados de 2005 a 2024

ID	Título/Referência	T/M/P/F/T	Framework (Y/N)	RQ	NE (A, I, IL)
S66	Hacia la Evaluación Automática de la Calidad de los Requerimientos de Software usando Redes Neuronales Long Short Term Memory [PS27]	Natural Language Processing (NLP), Recurrent Neural Networks (RNNs), Data Preprocessing, Classification, Labeling Process, Pre-sequence Padding, ISO/IEC/IEEE 29148:2018, Stanford POS Tagger	Y	1, 3, 4	0 - A
S67	The Politics of Privacy Theories: Moving from Norms to Vulnerabilities [PS100]	Case studies and literature reviews	Y	1, 3, 4	0 - A
S68	Applying Acceptance Requirements to Requirements Modeling Tools via Gamification: A Case Study on Privacy and Security [PS34]	Gamification Techniques, Case Study, Human-Centered Design Approach, Acceptance Requirements Analysis Process, Context-Based Analysis, Agon Framework, STS-Tool	Y	1, 4	0 - I
S69	Towards a privacy-enhancing tool based on de-identification methods [PS118]	De-identification techniques, k-anonymity, l-diversity, t-closeness, and differential privacy	Y	1, 4	0 - I
S70	The use of de-identification methods for secure and privacy-enhancing big data analytics in cloud environments [PS101]	De-identification, Homomorphic Encryption, Partial Encryption,	N	1, 3, 4	0 - A

Tabela A.1 – Estudos selecionados de 2005 a 2024

ID	Título/Referência	T/M/P/F/T	Framework (Y/N)	RQ	NE (A, I, IL)
S71	Using the design thinking empathy phase as a facilitator in privacy requirements elicitation [PS35]	Interviews, Surveys, Empathy Map, Brainstorm, Service Blueprint, Personas, Interview, Wireframe, Rabiscoframe, Insight Cards, Heuristics, Usability Testing, Value Canvas, Customer Journey Map, Focus Group, Workshop, Exploratory Research, Mind Mapping and Prototyping.	N	1, 3, 4	68 - I
S72	A Practical Approach to Stakeholder-driven Determination of Security Requirements based on the GDPR and Common Criteria [PS119]	Threat Modeling, Risk Assessment, Required Matching Process	Y	1, 3, 4	0 - I
S73	Preserving digital privacy in e-participation environments: Towards GDPR compliance [PS36]	Secure Tropos methodology, Data Protection Impact Assessment, Iterative processes, Elicitation, PDCA model	Y	1, 3, 4	0 - A
S74	Developing an Integrated ISO 27701 and GDPR based Information Privacy Compliance Requirements Model [PS120]	Content Analysis, Mapping, Action Design Research (ADR), Extracting Compliance Requirements, Developing an Integrated Set of Compliance Requirements, Integrated Requirements Engineering Model	Y	3, 4	0 - I

Tabela A.1 – Estudos selecionados de 2005 a 2024

ID	Título/Referência	T/M/P/F/T	Framework (Y/N)	RQ	NE (A, I, IL)
S75	On privacy-aware eScience workflows [PS91]	Automatic Identification of Sensitive Parameters, Anonymity Degree Enforcement, K-Anonymization, Data Merging, Policy Enforcement	Y	1, 3, 4	0 - A
S76	Utilizing a privacy impact assessment method using metrics in the healthcare sector [PS40]	Privacy Impact Assessment (PIA) method, structured process for conducting privacy impact assessments	Y	1, 3, 4	0 - A
S77	A Pufferfish privacy mechanism for monitoring web browsing behavior under temporal correlations [PS97]	Privacy leakage computation model (PLCM)	Y	3, 4	0 - A
S78	A risk-based methodology for privacy requirements elicitation and control selection [PS44]	Attribute-based access control model, Natural language processing, First-order logic-based declarative framework, Privacy Impact Assessment (PIA), Privacy by Design, LINDDUN framework, Trust and privacy framework	Y	1, 3, 4	0 - A
S79	Agile Teams' Perception in Privacy Requirements Elicitation: LGPD's compliance in Brazil [PS102]	User Story, Use Case, Threat Poker, Design Thinking techniques, Systematic Literature Review	N	1, 2	70 - A

Tabela A.1 – Estudos selecionados de 2005 a 2024

ID	Título/Referência	T/M/P/F/T	Framework (Y/N)	RQ	NE (A, I, IL)
S80	ConfIs: A Tool for Privacy and Security Analysis and Conflict Resolution for Supporting GDPR Compliance through Privacy-by-Design [PS51]	Agile software development method, Tropos methodology, Mapping, identification of conflicts and conflict resolution, SecTro	Y - ConfIs	4	15 - A
S81	COPri v.2 — A core ontology for privacy requirements [PS54]	Ontology Development, Threat Assessment, Systematic Literature Review, Conceptualization Process, PREprocess Framework, Protégé and HermiT Reasoner, OntoGraf Plugin	Y - COPri v.2	1, 3, 4	16 - A
S82	P-STORE: Extension of STORE Methodology to Elicit Privacy Requirements [PS67]	P-STORE methodology, Privacy Oriented Software Development, Structured Analysis Framework for Privacy and The framework developed by Spiekermann & Cranor for considering privacy in software systems	Y - P-STORE	1	59 - A

Tabela A.1 – Estudos selecionados de 2005 a 2024

ID	Título/Referência	T/M/P/F/T	Framework (Y/N)	RQ	NE (A, I, IL)
S83	Precision health data: Requirements, challenges and existing techniques for data security and privacy [PS68]	Blockchain, Cryptography, Differential privacy, Trusted Execution Environment, Machine learning paradigms, Dynamic data masking, Data-sharing management, Pseudo-anonymity techniques Encryption and authentication systems Audit logs	Y	4	0 - A
S84	Secure and Privacy-Aware Blockchain Design: Requirements, Challenges and Solutions [PS17]	Homomorphic Encryption, t-closeness Mechanism, Comparative Analysis, Taxonomy of Attacks and Countermeasures, Transaction-Privacy Bitcoin Framework	Y	1, 3, 4	0 - A
S85	Especificação de Requisitos de Privacidade em Conformidade com a LGPD: Resultados de um Estudo de Caso [PS25]	conceptual models, catalogs of privacy-related concepts	Y	1, 3, 4	5 - I
S86	Mobile app privacy in software engineering research: A systematic mapping study [PS37]	Elicitation Techniques, Ethnographic Analysis Techniques, Static and Dynamic Code Analysis, Systematic Mapping Study, Problem Analysis Framework, Adaptive Privacy Framework	N	1, 3, 4	0 - A

Tabela A.1 – Estudos selecionados de 2005 a 2024

ID	Título/Referência	T/M/P/F/T	Framework (Y/N)	RQ	NE (A, I, IL)
S87	Privacy preservation in e-health cloud: taxonomy, privacy requirements, feasibility analysis, and opportunities [PS92]	Anonymity techniques, Statistical disclosure control techniques, Privacy-aware models, document analysis, comparative analysis, Privacy requirement identification, Comparative analysis, taxonomy framework	Y	1, 3, 4	0 - A
S88	Privacy-Preserving Continuous Event Data Publishing [PS95]	Group-Based Privacy Preservation Techniques, Anonymization Functions, Continuous Data Publishing, Attack Analysis	Y	1, 4	0 - A
S89	Assessing frameworks for eliciting privacy & security requirements from laws and regulations [PS105]	Behavioural Modelling, Systematic Analysis, Elicitation of Requirements, Comparative Analysis, Extraction of Requirements, Mapping Requirements, Privacy Compliance Verification Framework, Information Disclosure Suite	Y	1	25 - I
S90	Detecting privacy requirements from User Stories with NLP transfer learning models [PS57]	Deep Learning Techniques, Natural Language Processing, Transfer Learning methods, Machine Learning methods	N	1, 4	0 - A

Tabela A.1 – Estudos selecionados de 2005 a 2024

ID	Título/Referência	T/M/P/F/T	Framework (Y/N)	RQ	NE (A, I, IL)
S91	Evaluating a privacy requirements specification method by using a mixed-method approach: results and lessons learned [PS9]	Goal-oriented modeling techniques such as Secure Tropos, KAOS, iStar, Privacy Criteria Method (PCM), LINDDUN Method, Privacy SQUARE method, PriS methodology, Non-Functional Requirement Framework (NFR), Business Process Model and Notation (BPMN), UML profiles and diagrams	Y	4	50 - A
S92	Privacy by Sharing Autonomy - A Design-Integrating Engineering Approach [PS14]	Complex Event Processing Techniques, Behavior-Centered Integrated Design and Engineering Approach and Subject-Oriented Modeling, Privacy Management Processes, Elicitation and Structuring of Privacy Requirements, Integrative Framework for Privacy Protection, User-Centered Development and Adaptation Scheme and Subject-Oriented Modeling Framework	Y	4	0 - A

Tabela A.1 – Estudos selecionados de 2005 a 2024

ID	Título/Referência	T/M/P/F/T	Framework (Y/N)	RQ	NE (A, I, IL)
S93	Uma taxonomia para requisitos de privacidade e sua aplicação no Open Banking Brasil [PS26]	Goal-Based Requirements Analysis Method (GBRAM), Grounded Theory, Identification of Privacy Requirements, Classification of Requirements, Refinement of Requirements, LGPD, ISO/IEC 29100	Y	1, 3, 4	0 - I
S94	Diretrizes para apresentação de políticas de privacidade voltadas à experiência do usuário [PS85]	Heuristic Evaluation, Design Sprint, Literature Review, User Testing, Evaluation Process, Validation Process, Usability Testing Tools, Prototyping Tools	Y	1, 3, 4	9 - A
S95	Do Platforms Care About Your Child's Data? A Proposal of Legal Requirements for Children's Privacy and Protection [PS86]	Legal Requirement Analysis, Case Study Analysis, Data Protection Impact Assessments, Compliance Evaluation, Children's Rights-by-Design (CRbD)	Y	1, 3, 4	0 - A
S96	A catalog of quality criteria to guide the assessment of applications' privacy policies [PS87]	systematic literature review (SLR)	Y	3, 4	0 - A
S97	A framework for privacy and security requirements analysis and conflict resolution for supporting GDPR compliance through privacy-by-design. [PS32]	Requirements Elicitation, Conflict Resolution Techniques, SePTA (Security, Privacy, and Trust Approach), Nominal Focus Group Technique, ConfIS Framework, SecTro	Y	1, 3, 4	0 - A

Tabela A.1 – Estudos selecionados de 2005 a 2024

ID	Título/Referência	T/M/P/F/T	Framework (Y/N)	RQ	NE (A, I, IL)
S98	From User Stories to Data Flow Diagram for Privacy Awareness [PS33]	Natural Language Processing (NLP), Named Entity Recognition (NER), PA-DFD	Y	1, 3, 4	0 - A
S99	Towards privacy-aware software design in small and medium enterprises [PS93]	Mixed-methods approach, case studies, surveys, and systematic literature reviews, Unified Software Development Process (UP)	Y	1, 3, 4	0 - A
S100	Privacy by Design: A Microservices-Based Software Architecture Approach [PS94]	Privacy by Design	Y	1, 3, 4	0 - A
S101	User Configurable Privacy Requirements Elicitation in Cyber-Physical Systems [PS38]	Usage Dependent Analysis, MisUse Cases, modularization of use cases, LINDDUN privacy analysis framework	Y	1, 3	0 - A
S102	A taxonomy for mining and classifying privacy requirements in issue reports [PS1]	Natural Language Processing (NLP), Goal-Based Requirements Analysis Method (GBRAM), APEC Privacy Framework	Y	4	0 - I

Tabela A.1 – Estudos selecionados de 2005 a 2024

ID	Título/Referência	T/M/P/F/T	Framework (Y/N)	RQ	NE (A, I, IL)
S103	An empirical study of automated privacy requirements classification in issue reports [PS48]	Bag-of-Words (BoW), N-gram Inverse Document Frequency (N-gram IDF), Term Frequency-Inverse Document Frequency (TF-IDF), Word2Vec, Convolutional Neural Network (CNN), Bidirectional Encoder Representations from Transformers (BERT), Asia-Pacific Economic Cooperation (APEC) privacy framework	N	1, 4	0 - A
S104	Data Block Matrix and Hyperledger Implementation: Extending Distributed Ledger Technology for Privacy Requirements [PS106]	Data Block Matrix, Chameleon Hash Functions, Controlled Data Deletion, Access Control Mechanisms, Data Sharing and Management, Deletion Request Validation, Hyperledger Fabric, Permissioned Distributed Ledger, Legal and Policy Frameworks, Proof-of-Concept Applications, NIST Resources	Y	1, 3, 4	0 - I

Tabela A.1 – Estudos selecionados de 2005 a 2024

ID	Título/Referência	T/M/P/F/T	Framework (Y/N)	RQ	NE (A, I, IL)
S105	Data protection and privacy: a model for evidence management [PS55]	Design Science Research, Privacy By design, Panel of Experts Method, Digital Questionaire, Data Treatment Operations, Evaluation Process, Matrix Analisis	Y - COM. PRIVACY	1	6 - A
S106	Security and Privacy Requirements for the Metaverse: A Metaverse Applications Perspective [PS76]	Literature Review, Identification of Threats	Y	1, 3, 4	0 - A
S107	Um Modelo de Conceitos Relacionados à Privacidade de Dados Pessoais [PS84]	systematic literature review (SLR)	Y	1, 3	0 - A
S108	Análise de conformidade da LGPD nas Instituições Públicas de Ensino Superior no Brasil sob a perspectiva dos profissionais de TIC [PS29]	Card Sorting, Likert Scale, Survey Design, Pilot Testing, Data Collection, CMMI for Development, ISO 20000, ITIL Service Design, OWASP, CIS, NIST frameworks	N	1, 3, 4	34 - A
S109	Uma abordagem baseada no Catálogo de Requisitos Não Funcionais para conformidade à LGPD [PS30]	Elicitation of Requirements, Refinement of Requirements, NFR Framework, Requirements Management, Survey Tools	Y	1, 3, 4	0 - A
S110	ML-based Compliance Verification of Data Processing Agreements against GDPR [PS39]	Machine learning, GDPR, DlkAIo	Y	1, 3, 4	0 - A

Tabela A.1 – Estudos selecionados de 2005 a 2024

ID	Título/Referência	T/M/P/F/T	Framework (Y/N)	RQ	NE (A, I, IL)
S111	Mobile Application Privacy Risk Assessments from User-authored Scenarios [PS121]	Named entity recognition (NER)	Y	3, 4	0 - I
S112	Leveraging NLP Techniques for Privacy Requirements Engineering in User Stories [PS10]	Goal-oriented perspective, risk-based perspective, privacy impact assessment, AGILE method, PRIPARE methodology and P-STORE, Neural Language Processing (NLP)	Y	1, 3, 4	0 - A
S113	Security and Privacy in Solar Insecticidal Lamps Internet of Things: Requirements and Challenges [PS18]	Authentication Protocols, Data Integrity Verification: Provable Data Possession (PDP) and Proofs of Retrievability (PoR), GODIT technique, Elliptic Curve Cryptography (ECC Graph-Based Outlier Detection), Data Management, Control-Flow Attestation, Artificial Neural Networks (ANN)	N	4	0 - A
S114	Towards a taxonomy of privacy requirements based on the LGPD and ISO/IEC 29100 [PS22]	Systematic Literature Review (SLR), Goal-Based Requirements Analysis Method (GBRAM), Grounded Theory methodology, ProPAn tool	Y	1, 4	0 - I

Tabela A.1 – Estudos selecionados de 2005 a 2024

ID	Título/Referência	T/M/P/F/T	Framework (Y/N)	RQ	NE (A, I, IL)
S115	Privacy Requirements and Realities of Digital Public Goods [PS82]	Secure data storage mechanisms, Access control mechanisms, NIST, LINDDUN, APEC, Privacy By Design, GDPR, OneTrust, Osano	Y	1, 4	101 - A
S116	Towards a Holistic Privacy Requirements Engineering Process: Insights from a Systematic Literature Review [PS28]	Systematic literature review (SLR)	Y	1, 3, 4	0 - A
S117	Requisitos de Segurança e Privacidade em Startups: Um Estudo Empírico em uma Aplicação de Governança de Dados [PS117]	Risk Assessment Techniques, GARSP-SGD Method, Risk Identification and Evaluation Process	Y	1, 3, 4	5 - I
S118	Do Entendimento à Aplicação: Requisitos de Privacidade e a Visão dos Usuários sobre a LGPD [PS83]	Survey Design Techniques	N	1, 4	200 - A
S119	A natural language-based method to specify privacy requirements: an evaluation with practitioners [PS31]	Privacy Criteria Method, PCM Tool	Y	1, 3, 4	21 - I
S120	Patterns of Inquiry in a Community Forum for Legal Compliance with Privacy Law [PS88]	Grounded theory	Y	3, 4	0 - A
S121	Integrating Differential Privacy and Contextual Integrity [PS89]	Differential Privacy (DP), Swapping	Y	1, 3, 4	0 - A
S122	Design of a Privacy Taxonomy in Requirement Engineering [PS90]	Privacy taxonomy, Non-Functional Requirements (NFRs)	Y	1, 3, 4	0 - A

Tabela A.1 – Estudos selecionados de 2005 a 2024

ID	Título/Referência	T/M/P/F/T	Framework (Y/N)	RQ	NE (A, I, IL)
S123	Integrating Contextual Integrity in Privacy Requirements Engineering: A Study Case in Personal E-Health [PS96]	LINDDUN Framework, Privacy Requirements Engineering Process, Data Flow Diagrams	Y	1, 3, 4	0 - A
S124	Governance-Focused Classification of Security and Privacy Requirements from Obligations in Software Engineering Contracts [PS99]	Natural Language Processing (NLP) Preprocessing Techniques, Grounded Theory-Based Approach, Machine Learning-Based Classification, Cross-Validation and Hyperparameter Tuning	Y	1, 4	0 - A
S125	Learning to Rank Privacy Design Patterns: A Semantic Approach to Meeting Privacy Requirements [PS98]	Natural Language Processing (NLP), Learning-to-Rank (LeToR), Classification Models, 5-Fold Cross-Validation, Privacy Requirements Engineering (PRE), Annotation Phase, Learning-to-Rank (LeToR) framework	Y	1, 3, 4	0 - A