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

Técnicas, Métodos, Processos, Frameworks e Ferramentas para Requisitos de Privacidade: Uma Revisão Sistemática de Literatura

João Francisco Gomes Targino

Artigo apresentado como requisito parcial
para conclusão do Bacharelado em Ciência da Computação

Orientadora
Prof. Dr.a Edna Dias Canedo

Brasília
2025

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

Técnicas, Métodos, Processos, Frameworks e Ferramentas para Requisitos de Privacidade: Uma Revisão Sistemática de Literatura

João Francisco Gomes Targino

Artigo apresentada como requisito parcial
para conclusão do Bacharelado em Ciência da Computação

Prof. Dr.a Edna Dias Canedo (Orientadora)
CIC/UnB

Prof. Dr. Daniel de Paula Porto
(CIC,UnB)

Prof. Dr. Fábio Lúcio Lopes de Mendonça
(FT/ENE)

Prof. Dr. Marcelo Grandi Mandelli
Coordenador do Bacharelado em Ciência da Computação

Brasília, 10 de fevereiro de 2025

Dedicatória

Dedico este trabalho aos meus familiares, que foram o alicerce da minha jornada acadêmica. Agradeço especialmente à minha mãe Janete Gomes, meu pai Robson Alex, minha avó Rita Gomes, minha irmã Suzany Evelyn e minha tia Adalgiza Gomes, por estarem ao meu lado em cada etapa desse caminho, oferecendo apoio incondicional e palavras de incentivo, também à minha prima Aline Laís, por ter sido minha inspiração para escolher esse curso de graduação e me ajudar nos preparativos para a faculdade. Em memória de minha avó Maria Nalva, meu tio Raniere Adson e minhas tias Walmira Monteiro e Darcy Gomes, que, mesmo ausentes fisicamente hoje, me apoiaram sempre que puderam enquanto em vida, e estiveram presentes em meu coração em cada momento desta conquista. Também dedico a todos os amigos, os que me apoiaram desde o início da jornada, e aos que essa jornada me trouxe

Agradecimentos

Gostaria de expressar minha profunda gratidão aos professores que me acompanharam ao longo desta jornada. Em especial, agradeço à minha orientadora, Edna Dias Canedo, pela oportunidade de realizar este trabalho e pelo apoio constante. Agradeço também aos meus colegas de curso, que estiveram ao meu lado, compartilhando os desafios e conquistas desta trajetória. Um agradecimento especial para Stefano Luppi, cuja colaboração foi fundamental para que eu conseguisse a orientação deste TCC.

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: Engenharia de Requisitos (ER) depende da colaboração de vários papéis—tais qual, engenheiro de requisitos, *stakeholders*, e desenvolvedores—e várias técnicas, métodos, processos, *frameworks*, e ferramentas. Isso faz com que a ER seja um processo fortemente dependente do ser humano que se beneficia do suporte de ferramentas. Entender como essas técnicas, métodos, processos, *frameworks*, e ferramentas são aplicadas através das fases de ER podem fornecer percepções valiosas de caminhos para melhorar o processo de ER, contribuindo para resultados melhores. **Objetivo**: O objetivo primário deste estudo é identificar técnicas, métodos, processos, *frameworks*, e ferramentas aplicadas entre as diferentes fases de ER—tais quais elicitação, análise, especificação, validação, e gerenciamento—para atender os requisitos de privacidade. **Método** Foi conduzida uma Revisão Sistemática de Literatura e foram identificados 125 estudos, e também um questionário com 31 profissionais. **Resultados**: Foi identificada uma gama de técnicas, métodos, processos, frameworks, e ferramentas para atender os requisitos de privacidade. A maioria dos estudos foram conduzidos em contextos acadêmicos, com as ferramentas mais frequentes 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 dos requisitos de privacidade. Na indústria, a maioria das técnicas identificadas na literatura não são conhecidas ou usadas pelo profissionais. **Conclusão**: Esse estudo apresenta uma análise compreensiva das técnicas e ferramentas para os requisitos de privacidade na ER, revelando um forte foco no contexto acadêmico e com aplicação limitada na indústria. Pesquisas futuras devem explorar a escalabilidade e efetividade dessas ferramentas nos cenários reais, bem como as razões dos profissionais não as utilizarem.

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

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**: A Systematic literature review (SLR) was conducted and identified 125 primary studies, and we also conducted a survey with 31 practitioners. **Results**: The review identified a range of techniques, methods, processes, frameworks, and tools for addressing privacy requirements. Most studies were conducted in academic contexts, with the most frequently used tools being: PriS Method, Secure Tropos, LINDDUN, i* (i-star), STRAP (Structured Analysis for Privacy), Privacy by Design (PbD), and SQUARE. Additionally, over 75% of the studies applied these tools in the privacy requirements elicitation phase. In the industry, most of the techniques identified in the literature are not known or used by practitioners. **Conclusion:**This study provides a comprehensive analysis of techniques and tools for privacy requirements in RE, revealing a strong focus on academic contexts with limited industry application. Future research should explore the scalability and effectiveness of these tools in real-world environments, as well as the reasons why practitioners do not use them.

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

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Abreviaturas e Siglas

ER Engenharia de Requisitos.

GDPR General Data Protection Regulation.

IA Inteligência Artificial.

LGPD Lei Geral de Proteção de Dados.

QA Avaliação de Qualidade.

RQs Questões de Pesquisa.

RSL Revisão Sistemática de Literatura.

Capítulo 1

Introdução

Nos dias de hoje, onde há o grande crescimento do mundo digital, a privacidade tornou-se uma preocupação central no desenvolvimento de software [1, 2]. Com o volume de dados pessoais processados por aplicações e sistemas crescendo, garantir a privacidade é um requisito legal e uma responsabilidade ética fundamental. O desafio de integrar a privacidade no desenvolvimento de software está em identificar técnicas, métodos, processos, *frameworks*, e ferramentas que podem efetivamente atender às preocupações de privacidade através do processo de desenvolvimento [3, 4].

A privacidade deve ser considerada em todos os estágios, desde a elicitação e gerenciamento de requisitos até os estágios finais do desenvolvimento e implementação, para prevenir riscos potenciais, brechas e não conformidades com regulamentação como *General Data Protection Regulation (GDPR)* [5] e Lei Geral de Proteção de Dados (LGPD) [6]. Além disso, o interesse em sistemas baseados em Inteligência Artificial (IA) vem crescendo rapidamente, tanto dentro do desenvolvimento de software como na sociedade em geral. Como resultado, as preocupações sobre privacidade têm crescido na mesma velocidade [1, 2].

As tecnologias que utilizam da Inteligência Artificial (IA) estão cada vez mais integradas em várias aplicações, desde serviços personalizados até análise preditiva, esses são alguns dos motivos pelos quais uma grande quantidade de dados sensíveis é processada, aumentando significativamente os desafios sobre privacidade e segurança. Isso intensifica a necessidade de medidas robustas de privacidade e designs preocupados com a privacidade nos sistemas de IA para garantir que os dados do usuário sejam tratados com responsabilidade e em conformidade com a evolução das regulamentações [2]. Um dos aspectos mais importantes para atender às preocupações de privacidade no desenvolvimento de software é a aplicação efetiva de Técnicas de Engenharia de Requisitos. Principalmente, entendendo e aplicando técnicas existentes do campo da Engenharia de Requisitos, como elicitação, especificação, validação e gerenciamento, são essenciais para garantir que os re-

quisitos de privacidade estão definidos adequadamente, priorizados e incorporados dentro do design do sistema. Essas técnicas fornecem abordagens estruturadas para identificar as necessidades de privacidade, avaliando riscos potenciais e garantindo a privacidade durante todo o processo de desenvolvimento [3].

Outro problema é que privacidade possui várias definições na literatura e todas convergem para o mesmo princípio fundamental. Westin [7] define a privacidade como a reivindicação de indivíduos, grupos ou instituições de determinar por si mesmos quando, como e até que ponto as informações sobre eles são comunicadas a outros. Pfleeger e Charles [8] definem privacidade como o conhecimento sobre a pessoa em termos de comunicação e atividades, logo, o direito de controlar quem sabe certos aspectos sobre a pessoa, sua comunicação e suas atividades. Outros pesquisadores definem privacidade como uma autonomia pessoal, significando a liberdade de revelar a própria identidade e preferências sem o medo de perseguição ou interferência indesejada [9]. Em Ciência da Computação, privacidade é comumente igualada a sigilo ou confidencialidade e pode ser acessada através de controles de acesso e mecanismos de encriptação [9].

Para garantir que o software protege adequadamente os dados do usuário, é necessário definir requisitos de privacidade durante as fases de engenharia de requisitos. Esses requisitos de privacidade devem ser baseados no destino dos dados do usuário [10] [11], ou mesmo baseados em aspectos sociais de privacidade através de análise comportamental [12]. Requisitos de privacidade geralmente estão alinhados com a legislação de privacidade ou regulamentações em certos países [3]. Entre os *frameworks* legais atuais estão General Data Protection Regulation (GDPR) [5] e Lei Geral de Proteção de Dados (LGPD) [6] [13, 14]. Para um projeto de desenvolvimento de software cumprir essas regulamentações, requisitos de privacidade devem garantir a proteção dos dados do usuário em todos os sistemas desenvolvidos pelas organizações [15].

Requisitos de privacidade abordam as preocupações de privacidade, garantindo que os padrões de privacidade de um sistema de software sejam suportados e atendidos. Requisitos de privacidade devem garantir privacidade de dados introduzindo retorno apropriado e mecanismos de controle, permitindo aos usuários melhor controle sobre a informação ligada a ameças à privacidade [16]. Os tipos de requisitos de privacidade encontrados na literatura incluem [17]: 1) Anonimização - permite que entidades usem recursos ou serviços de uma aplicação sem precisar revelar sua identidade; 2) Desvinculação - garante que uma entidade use um serviço sem ser associada com ele; 3) Pseudonimização - dá aos usuários do sistema liberdade para operaram sobre um pseudônimo ou pseudônimos sem ter que entregar informações pessoais que possam revelar sua identidade; 4) Inobservância - previne qualquer entidade de saber com certeza que um usuário está acessando um serviço e garante que as ações do usuário não estão sendo monitoradas enquanto usa uma

serviço ou um recurso; e 5) Indetectabilidade - Garante que uma entidade não consiga identificar qual usuário, de um conjunto de usuários, está acessando o serviço.

O processo de engenharia de privacidade no ciclo de desenvolvimento de software começa identificando e definindo os requisitos de privacidade [18]. Essa fase é particularmente desafiadora devido à complexidade das leis de privacidade e a necessidade de equilibrar as preocupações de privacidade com outros requisitos concorrentes. Para desenhar e implementar sistemas de preservação de privacidade efetivamente, técnicas robustas, métodos, *frameworks* e ferramentas são essenciais. Engenharia de privacidade envolve várias abordagens, incluindo usar regulamentações para estabelecer requisitos de privacidade e avaliar os ativos organizacionais para atender às necessidades de privacidade [18].

Foi conduzida uma Revisão Sistemática de Literatura (RSL) e uma pesquisa para explorar e identificar as técnicas, métodos, processos, *frameworks* e ferramentas empregadas na literatura e na indústria para realizar a elicitação de requisitos, análise, especificação, validação, e gerenciamento relacionado com os requisitos de privacidade. A RSL revelou que *SQUARE, Secure Tropos, PriS, i* (i-Star), LINDDUN, STRAP, e Privacy by Design* são as técnicas mais comumente utilizadas. A maioria dessas técnicas aplica-se exclusivamente à fase de elicitação de requisitos.

Capítulo 2

Contexto e Trabalhos Relacionados

A privacidade é considerada um conceito multifacetado e dinâmico, indo além do simples controle sobre as informações pessoais dos indivíduos [19]. Privacidade refere-se ao direito fundamental de cada indivíduo de gerenciar suas informações e decidir como, quando e com quem esses dados serão compartilhados [20]. A privacidade contemporânea não se limita apenas à proteção contra a vigilância estatal ou corporativa, mas abrange também a capacidade de autodeterminação informacional [21].

Veseli *et al.* [22] 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, sobre as informações contidas nos mesmos; 2) *Recipient sphere* – se refere ao contexto das organizações, onde o engenheiro de software tem a responsabilidade de minimizar os riscos de vazamento de dados confidenciais, junto aos riscos de quebra de privacidade; e 3) *Joint sphere* – que consiste nas companhias que detêm dados pessoais dos indivíduos, onde, de maneira semelhante 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.

Em 2005 Kalloniatis *et al.* [20] já alertava 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 foi tentar harmonizar internacionalmente as legislações de privacidade. Porém, um dos contrapontos é que seria muito difícil de alcançar, principalmente pelas diferenças culturais. Hoje existem aspectos parecidos nas legislações de cada país, porém, não é possível existir somente uma única legislação para todos.

A Lei Geral de Proteção de Dados (LGPD) [6], 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 pela General Data Protection Regulation (GDPR) [5], possui como objetivo principal a proteção dos direitos fundamentais de liberdade e privacidade, assegurando a transparência no uso de informações pessoais.

A LGPD [6] e a GDPR [5] compartilham diversos princípios, dando ênfase à transparência, necessidade, segurança e o propósito específico do uso de dados. Além disso, essas regulamentações garantem aos indivíduos direitos semelhantes, como o acesso, correção, deleção e portabilidade dos seus dados, bem como o direito de ser informado sobre o uso e o compartilhamento da sua informação.

Complementando os princípios de privacidade estabelecidos na LGPD [6], em [23] foram propostos padrões de privacidade em conformidade com a lei, baseados em entrevistas com profissionais de TI. Isso surgiu da necessidade de criar padrões para identificar princípios e garantir conformidade com as regulamentações de privacidade aplicáveis.

Em [13] é proposta uma taxonomia de requisitos de privacidade para apoiar equipes de desenvolvimento de software a superar os desafios de conformidade com a lei, principalmente aqueles relacionados à LGPD e à ISO/IEC 29100. Utilizando uma Revisão Sistemática de Literatura, as autoras identificaram 10 estudos primários como base para o trabalho. Por meio do Método de Análise de Requisitos Baseado em Objetivos (GBRAM) e da Teoria Fundamentada (Grounded Theory), formulam 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 desenvolvimento de software na especificação efetiva dos requisitos de privacidade.

Em [24] foi desenvolvida uma ferramenta automatizada para otimizar a análise e implementação dos princípios da LGPD, com foco em auxiliar organizações na garantia da conformidade com os requisitos de privacidade estabelecidos 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.

Já em [25] foi proposto um catálogo de padrões de privacidade e um guia denominado G-Priv, com o objetivo de auxiliar na especificação de requisitos de privacidade em conformidade com a LGPD. Para avaliar o G-Priv, os autores aplicaram um questionário com 18 profissionais, que consideraram o guia fácil de compreender, especialmente na definição de funções e responsabilidades dos stakeholders envolvidos nos quatro estágios do processo. Os participantes da pesquisa também destacaram a usabilidade e eficiência do guia, considerando-o uma ferramenta valiosa para apoiar analistas de requisitos na

especificação de requisitos de privacidade alinhados à Lei Geral de Proteção de Dados (LGPD).

Requisitos de privacidade referem-se às condições, padrões e regulamentações que protegem os dados pessoais e resguardam os direitos individuais de privacidade. Esses requisitos geralmente surgem de *frameworks* legais, como a GDPR e a LGPD. Eles têm como foco definir como os dados pessoais devem ser coletados, processados, armazenados e distribuídos, garantindo transparência, responsabilização e o direito à privacidade dos indivíduos [3].

O objetivo principal da Engenharia de Requisitos (ER) é definir claramente e compreender os requisitos de privacidade dos sistemas, garantindo sua integração fluida no design e desenvolvimento. Esse processo geralmente envolve a condução de análises de risco, avaliações de ameaças e avaliações de impacto à privacidade para identificar e tratar potenciais riscos à privacidade.

Após os requisitos de privacidade serem identificados e definidos, o foco passa a ser o desenvolvimento de soluções que atendam a esses requisitos, um processo conhecido como engenharia de design de privacidade. Essa fase pode envolver a implementação de tecnologias específicas ou estratégias, como criptografia ou anonimização, para garantir a privacidade dos dados e dos usuários. Adotar uma abordagem baseada em risco garante que os designs de privacidade estejam alinhados aos princípios estabelecidos da gestão de risco [18].

Requisitos de privacidade são frequentemente tratados como requisitos não funcionais, enfrentando desafios semelhantes a outros tipos de requisitos, como a falta de documentação adequada e o risco de serem negligenciados no processo de desenvolvimento. Outro problema comum é a formulação incompleta, o que pode prejudicar a clareza do projeto. Além disso, a definição de requisitos de privacidade frequentemente envolve normas legais, o que complica o trabalho dos analistas de sistemas, que muitas vezes não possuem a familiaridade necessária com a interpretação jurídica [26].

A maioria dos trabalhos existentes sobre requisitos de privacidade trata esses requisitos como simples requisitos não funcionais, sem oferecer técnicas específicas para sua implementação [27]. Além disso, muitos os abordam sob a ótica dos requisitos de segurança, com foco predominante em aspectos como confidencialidade, deixando de lado questões igualmente importantes, como anonimato, pseudonimato, desvinculação e inobservância, entre outras.

Existem diversas técnicas para especificar os requisitos de privacidade. Esse tema foi abordado em [28] sob duas perspectivas: uma abordagem orientada a metas e uma abordagem orientada a riscos. A abordagem orientada a metas foca em derivar os princípios de privacidade e estabelecê-los como requisitos do sistema. As metas de privacidade ou

de proteção de dados são comumente derivadas de princípios fundamentais de privacidade e *frameworks* legais.

Hansen *et al.* [29] identificaram seis metas principais de proteção de dados: confidencialidade, integridade, disponibilidade, desvinculação, transparência e intervenção.

A tríade CIA — Confidencialidade, Integridade e Disponibilidade — é um *framework* amplamente reconhecido para definir e avaliar requisitos de segurança e serve como base para a segurança da informação. A tríade CIA pode ser adaptada para atender aos requisitos específicos de privacidade e regulamentação na proteção de dados. Com base nessas seis metas, foi desenvolvida uma metodologia de Engenharia de Requisitos de Privacidade como parte do método ProPAn, integrando essas metas para tratar de forma abrangente a privacidade e a proteção de dados [30].

Diversas metodologias contribuíram para o corpo de conhecimento, incluindo métodos, ferramentas, bases de conhecimento sobre privacidade, modelos, documentação e outros elementos projetados para ajudar os engenheiros de software a criar sistemas que preservem a privacidade. Foi enfatizada em [31] a necessidade urgente de uma pesquisa mais aprofundada para identificar métodos que auxiliem no desenvolvimento de sistemas focados na privacidade dos dados. Os autores destacam a importância de ferramentas autônomas para uma adoção mais ampla na indústria.

Esta pesquisa aborda essa lacuna, investigando as técnicas, métodos, processos, *frameworks* e ferramentas utilizadas na Engenharia de Requisitos (ER) para elicitação, análise, especificação, validação e gerenciamento dos requisitos de privacidade.

Capítulo 3

Revisão Sistemática de Literatura

Neste trabalho, foi realizada uma Revisão Sistemática de Literatura, também conhecida como revisão sistemática, segundo o protocolo proposto por Kitchenham *et al.* [32]. 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 RSL 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 [32].

Kitchenham *et al.* [32] divide a RSL 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.
- **Relato**: Consiste em especificar mecanismos de disseminação de resultados, juntamente da formação e análise do relatório principal referente a revisão realizada.

3.1 String de Busca

Para a execução da RSL, foi inicialmente definida uma *string* de busca conforme o conjunto de critérios PICO [33], 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.
- **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.

3.2 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 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*) [34] 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

Base de Dados	String de Busca
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

utilizadas na indústria, foram considerados os métodos de avaliação de eficácia e testes realizados em ambientes reais.

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 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

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

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.

3.3 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.* [32]. 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 3.1.

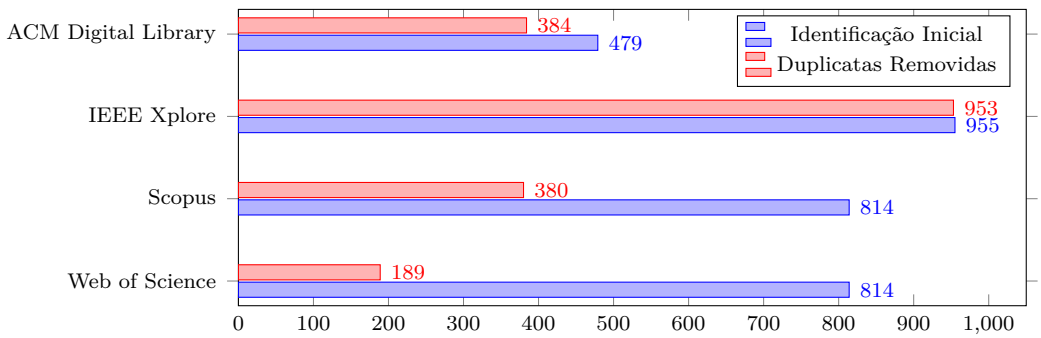

Figura 3.1: Quantidade de Estudos Identificados e Selecionados por Base de Dados Digital

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 3.1.

3.4 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 3.5;
- Accepted: O artigo atende aos requisitos.

3.5 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.

3.6 Condução da RSL

Ao longo do processo da RSL, 1904 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), (Requirementes Engineering Conference) e (REFSQ), totalizando 125 artigos classificados como aceitos ao fim desta revisão.

A Figura 3.2 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 à 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.

3.7 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 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.

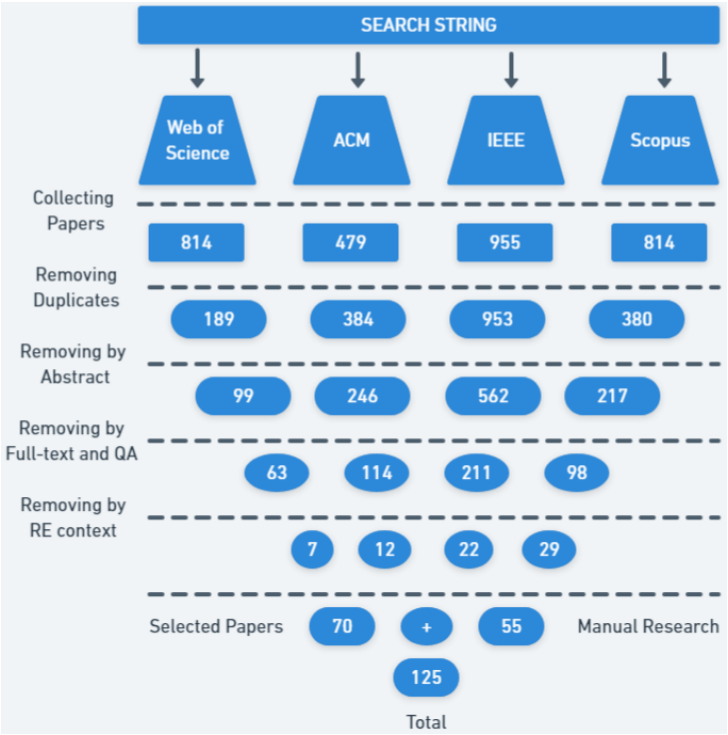

Figura 3.2: Etapas do processo de seleção dos estudos

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.

Tabela 3.3: Estudos selecionados.

ID	Título do Estudo	ID	Título do Estudo
[35]	A Data-Driven Approach to Designing for Privacy in Household IoT	[36]	A foundation for requirements analysis of privacy preserving software
[37]	A privacy threat analysis framework: Supporting the elicitation and fulfillment of privacy requirements	[38]	A risk-based methodology for privacy requirements elicitation and control selection
[39]	A security requirements modelling language for cloud computing	[40]	A semi-automatic approach for eliciting cloud security and privacy requirements

[41]	A Study of Privacy Requirements for Smart toys	[42]	A taxonomy for mining and classifying privacy requirements in issue reports
[43]	Adapting the SQUARE Process for Privacy Requirements Engineering	[44]	Addressing privacy requirements in system design: the PriS method
[45]	Agile Teams' Perception in Privacy Requirements Elicitation: LGPD's compliance in Brazil	[46]	Aligning security and privacy to support the development of secure information systems
[47]	An empirical study of automated privacy requirements classification in issue reports	[48]	Applying Soft Computing Technologies for Implementing Privacy-Aware Systems
[49]	Appropriate Technical and Organizational Measures Identifying Privacy Engineering Approaches to Meet GDPR Requirements	[50]	Assessing frameworks for eliciting privacy & security requirements from laws and regulations
[51]	Assurance of Security and Privacy Requirements for Cloud Deployment Models	[52]	Comparing Privacy Requirements Engineering Approaches
[53]	Computer-Aided Privacy Requirements Elicitation Technique	[54]	ConfIs: A Tool for Privacy and Security Analysis and Conflict Resolution for Supporting GDPR Compliance through Privacy-by-Design
[55]	Conflicts Between Security and Privacy Measures in Software Requirements Engineering	[56]	COPri - A Core Ontology for Privacy Requirements Engineering
[57]	COPri v.2 - A core ontology for privacy requirements	[58]	Data Block Matrix and Hyperledger Implementation: Extending Distributed Ledger Technology for Privacy Requirements
[59]	Data protection and privacy: a model for evidence management	[20]	Dealing with privacy issues during the system design process

[60]	Design of a Privacy Taxonomy in Requirement Engineering	[61]	Designing privacy-aware internet of things applications
[62]	Detecting privacy requirements from User Stories with NLP transfer learning models	[21]	Early Privacy: Approximating Mental Models in the Definition of Privacy Requirements in Systems Design
[63]	Eddy, a formal language for specifying and analyzing data flow specifications for conflicting privacy requirements	[64]	Elicitation of Privacy Requirements for the Internet of Things Using ACCESSORS
[65]	Eliciting security requirements with misuse cases	[66]	Enforcement of privacy requirements
[67]	Engineering Privacy	[22]	Engineering Privacy by Design - Lessons from the Design and Implementation of an Identity Wallet Platform
[68]	Engineering privacy requirements valuable lessons from another realm	[69]	Evaluating a privacy requirements specification method by using a mixed-method approach: results and lessons learned
[70]	Evaluating cloud deployment scenarios based on security and privacy requirements	[71]	Evaluation of a security and privacy requirements methodology using the physics of notation
[72]	Framework and Requirements for Reconciling Digital Services and Privacy	[73]	GDPR Transparency Requirements and Data Privacy Vocabularies
[74]	Identifying Privacy Functional Requirements for Crowdsourcing Applications in Smart Cities	[75]	Incorporating privacy requirements into the system design process: The PriS conceptual framework
[76]	Integrating privacy requirements considerations into a security requirements engineering method and tool	[77]	Leveraging NLP Techniques for Privacy Requirements Engineering in User Stories

[78]	Modeling Security and Privacy Requirements: a Use Case-Driven Approach	[79]	Modelling the interplay of security, privacy and trust in sociotechnical systems: a computer-aided design approach
[80]	P-STORE: Extension of STORE Methodology to Elicit Privacy Requirements	[81]	PCM Tool: Privacy Requirements Specification in Agile Software Development
[82]	Perceptions of ICT practitioners regarding software privacy	[83]	Precision health data: Requirements, challenges and existing techniques for data security and privacy
[84]	Preprocess before You Build: Introducing a Framework for Privacy Requirements Engineering	[85]	Pris Tool: A Case Tool For Privacy Oriented Requirements Engineering
[86]	Privacy by Design in Federated Identity Management	[87]	Privacy by Sharing Autonomy - A Design-Integrating Engineering Approach
[88]	Privacy Control Patterns for Compliant Application of GDPR	[89]	Privacy Requirements: Findings and Lessons Learned in Developing a Privacy Platform
[90]	Privacy Requirements: Present & Future	[91]	Privacy-enhanced BPMN: enabling data privacy analysis in business processes models
[92]	Privacy-Enhanced System Design Modeling Based on Privacy Features	[93]	Privacy, security, legal and technology acceptance elicited and consolidated requirements for a GDPR compliance platform
[94]	Integrating Differential Privacy and Contextual Integrity	[95]	privacyTracker: A Privacy-by-Design GDPR-Compliant Framework with Verifiable Data Traceability Controls
[96]	Protecting privacy in system design: The electronic voting case	[97]	Recommender-based Privacy Requirements Elicitation - EPICUREAN

[98]	Secure and Privacy-Aware Blockchain Design: Requirements, Challenges and Solutions	[99]	Secure Tropos: A Security-Oriented Extension of the Tropos Methodology
[100]	Security and Privacy in Solar Insecticidal Lamps Internet of Things: Requirements and Challenges	[101]	From User Stories to Data Flow Diagram for Privacy Awareness
[102]	Security and Privacy Requirements Engineering Methods for Traditional and Cloud-Based Systems: A Review	[103]	Security and Privacy Requirements for the Metaverse: A Metaverse Applications Perspective
[104]	Specifying privacy requirements with goal-oriented modeling languages	[105]	STRAP: A Structured Analysis Framework for Privacy
[106]	Supporting the design of privacy-aware business processes via privacy process patterns	[107]	The Grace Period Has Ended: An Approach to Operationalize GDPR Requirements
[108]	Tool-Supporting Data Protection Impact Assessments with CAIRIS	[109]	Towards a Catalog of Privacy Related Concepts
[110]	Towards a framework to elicit and manage security and privacy requirements from laws and regulations	[111]	Towards a Risk-Driven Methodology for Privacy Metrics Development
[112]	Towards a taxonomy of privacy requirements based on the LGPD and ISO/IEC 29100	[19]	Towards an Ontology for Privacy Requirements via a Systematic Literature Review
[113]	Towards Detecting and Mitigating Conflicts for Privacy and Security Requirements	[114]	Towards the Design of Usable Privacy by Design Methodologies
[115]	TrUStAPIS: a trust requirements elicitation method for IoT	[116]	Us and them: a study of privacy requirements across north america, asia, and europe

[117]	Using Privacy Process Patterns for Incorporating Privacy Requirements into the System Design Process	[23]	Especificação de Requisitos de Privacidade em Conformidade com a LGPD: Resultados de um Estudo de Caso
[26]	Uma taxonomia para requisitos de privacidade e sua aplicação no Open Banking Brasil	[118]	Hacia la Evaluación Automática de la Calidad de los Requerimientos de Software usando Redes Neuronales Long Short Term Memory
[119]	Privacy Requirements and Realities of Digital Public Goods	[120]	Do Entendimento à Aplicação: Requisitos de Privacidade e a Visão dos Usuários sobre a LGPD
[27]	Um Modelo de Conceitos Relacionados à Privacidade de Dados Pessoais	[121]	Análise de conformidade da LGPD nas Instituições Públicas de Ensino Superior no Brasil sob a perspectiva dos profissionais de TIC
[122]	Uma abordagem baseada no Catálogo de Requisitos Não Funcionais para conformidade à LGPD	[123]	Diretrizes para apresentação de políticas de privacidade voltadas à experiência do usuário
[124]	Do Platforms Care About Your Child's Data? A Proposal of Legal Requirements for Children's Privacy and Protection	[125]	A catalog of quality criteria to guide the assessment of applications' privacy policies
[126]	A natural language-based method to specify privacy requirements: an evaluation with practitioners	[127]	Patterns of Inquiry in a Community Forum for Legal Compliance with Privacy Law
[128]	A framework for privacy and security requirements analysis and conflict resolution for supporting GDPR compliance through privacy-by-design.	[129]	Requisitos de Segurança e Privacidade em Startups: Um Estudo Empírico em uma Aplicação de Governança de Dados

[130]	Towards a Holistic Privacy Requirements Engineering Process: Insights from a Systematic Literature Review	[131]	The Politics of Privacy Theories: Moving from Norms to Vulnerabilities
[132]	Applying Acceptance Requirements to Requirements Modeling Tools via Gamification: A Case Study on Privacy and Security	[133]	Towards a privacy-enhancing tool based on de-identification methods
[134]	The use of de-identification methods for secure and privacy-enhancing big data analytics in cloud environments	[135]	Using the design thinking empathy phase as a facilitator in privacy requirements elicitation
[136]	A Practical Approach to Stakeholder-driven Determination of Security Requirements based on the GDPR and Common Criteria	[137]	Preserving digital privacy in e-participation environments: Towards GDPR compliance
[138]	Developing an Integrated ISO 27701 and GDPR based Information Privacy Compliance Requirements Model	[139]	On privacy-aware eScience workflows
[140]	Mobile app privacy in software engineering research: A systematic mapping study	[141]	Privacy preservation in e-health cloud: taxonomy, privacy requirements, feasibility analysis, and opportunities
[142]	Towards privacy-aware software design in small and medium enterprises	[143]	Privacy by Design: A Microservices-Based Software Architecture Approach
[144]	User Configurable Privacy Requirements Elicitation in Cyber-Physical Systems	[145]	Privacy-Preserving Continuous Event Data Publishing
[146]	Integrating Contextual Integrity in Privacy Requirements Engineering: A Study Case in Personal E-Health	[147]	ML-based Compliance Verification of Data Processing Agreements against GDPR

[148]	Mobile Application Privacy Risk Assessments from User-authored Scenarios	[149]	Utilizing a privacy impact assessment method using metrics in the healthcare sector
[150]	A Pufferfish privacy mechanism for monitoring web browsing behavior under temporal correlations	[151]	Governance-Focused Classification of Security and Privacy Requirements from Obligations in Software Engineering Contracts
[152]	Learning to Rank Privacy Design Patterns: A Semantic Approach to Meeting Privacy Requirements		

Durante a extração, foi possível observar um padrão de publicações ao longo dos anos, assim como ilustrado na Figura 3.3. Com base nesses dados, foi possível concluir que houve uma baixa produção inicial nos anos de 2005 a 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 General Data Protection Regulation (GDPR) [5] e Lei Geral de Proteção de Dados (LGPD) [6] terem sido aprovadas e entrarem em vigor durante este período.

Critérios de Extração

Os critérios de extração de dados foram definidos com o objetivo de responder às questões de pesquisa estabelecidas e cobrir todos os aspectos relevantes da literatura e da indústria relacionados aos requisitos de privacidade. Os critérios foram organizados em formato de campos em um formulário de extração, onde cada artigo selecionado teve suas principais informações extraídas e armazenadas em cada seção, para fácil acesso. Os campos apresentados na Tabela 3.4 foram gerados com base no formulário proposto em por Hidellaarachchi *et al.* [153]:

Tabela 3.4: Formulário de Extração de Dados

ID	Extraction Criteria
1	Study ID

2	Source Type
3	Paper Title
4	Published Year
5	The number of citations of the study?
6	What is the aim/motivation/goal of the study?
7	What research question does the study answer?
8	Subjects used in the study: Professionals or Undergraduates (Requirement Engineers/ Stakeholders/ Clients/ Students)?
9	What are the TECHNIQUES that are considered in the study?
10	What are the METHODS that are considered in the study?
11	What are the PROCESSES that are considered in the study?
12	What are the FRAMEWORKS that are considered in the study?
13	What are the TOOLS that are considered in the study?
14	What are the other things (not techniques, methods, processes, frameworks and tools) that are considered in the study?
15	What phases of the RE are considered in the study (Elicitation/ Specification/ Analysis/ Validation/ Management)?
16	Does the research identify the most affected RE phase by privacy requirements? (Yes/ No)
17	If Yes, What is the most affected RE Phase(s)?
18	Does the study use any existing domain models related to privacy requirements? (Yes/ No)
19	If yes, what are the existing domain models used in studies to identify privacy requirements?
20	Method used in the study(s)? (Case studies/Interviews/ Modelling /framework/ Document analysis/ surveys/ other)
21	Is the study conducted based on academia or industry?
22	The number of participants used in the study
23	What type of data analysis used in the study? (Qualitative/ Quantitative/ Mixed)
24	What are the key research gaps/ future work identified by each study?
25	Does the research focus on identifying the relationship between different privacy requirements? (Yes/ No)
26	If Yes, what are the identified relationships between different privacy requirements?

27	Does the research include how the privacy requirements impact on RE? (Yes/ No)
28	If Yes, what is the nature of the impact of the privacy requirements on RE? (Positive/ Negative/ Both)
29	If Positive, does the study mention the benefits of considering the privacy requirements?
30	If Negative, how it will impact on RE?
31	Does the study suggest any approach to mitigate the negative impact?
32	Main outcome/Results of the study?
33	Does the study come up with a framework/ model as the final outcome?
34	If Yes, what type of framework it is? (Elaborate the developed framework)
35	How do they evaluate their results/ framework/ model?
36	What are the major recommendations of the study?

3.8 Resultados

Baseando-se nos critérios de seleção apresentados anteriormente, os dados dos 125 estudos aceitos foram extraídos de forma clara e objetiva por meio do formulário de extração. Esses resultados possibilitaram estabelecer a relação entre todos os artigos e as questões de pesquisa, além de identificar as técnicas, métodos, processos, *frameworks* e ferramentas utilizados no processo de elicitação dos requisitos de privacidade e, consequentemente, na Engenharia de Requisitos.

É importante destacar que alguns estudos não forneceram dados suficientemente claros para preencher todos os campos do formulário de extração. No entanto, isso não foi considerado uma limitação, pois os critérios de qualidade já haviam sido aplicados aos estudos aceitos.

A Figura 3.4 apresenta a quantidade de estudos conforme o método utilizado pelos estudos selecionados. O método mais frequente foi o *Estudo de Caso*, com um total de 29 estudos primários que empregaram *frameworks* para abordar os requisitos de privacidade. Em seguida, a análise de documentação foi o segundo método mais utilizado, com 22 estudos. Tanto *frameworks* quanto modelagem foram adotados em 20 estudos cada. Além disso, 15 estudos utilizaram pesquisas, enquanto 10 empregaram outros métodos não especificados. Por fim, 8 estudos utilizaram entrevistas como método primário.

Dos 125 estudos primários, 40 focaram em uma das fases de Engenharia de Requisitos, apresentando ferramentas específicas para as respectivas fases, ou indicando como os seus

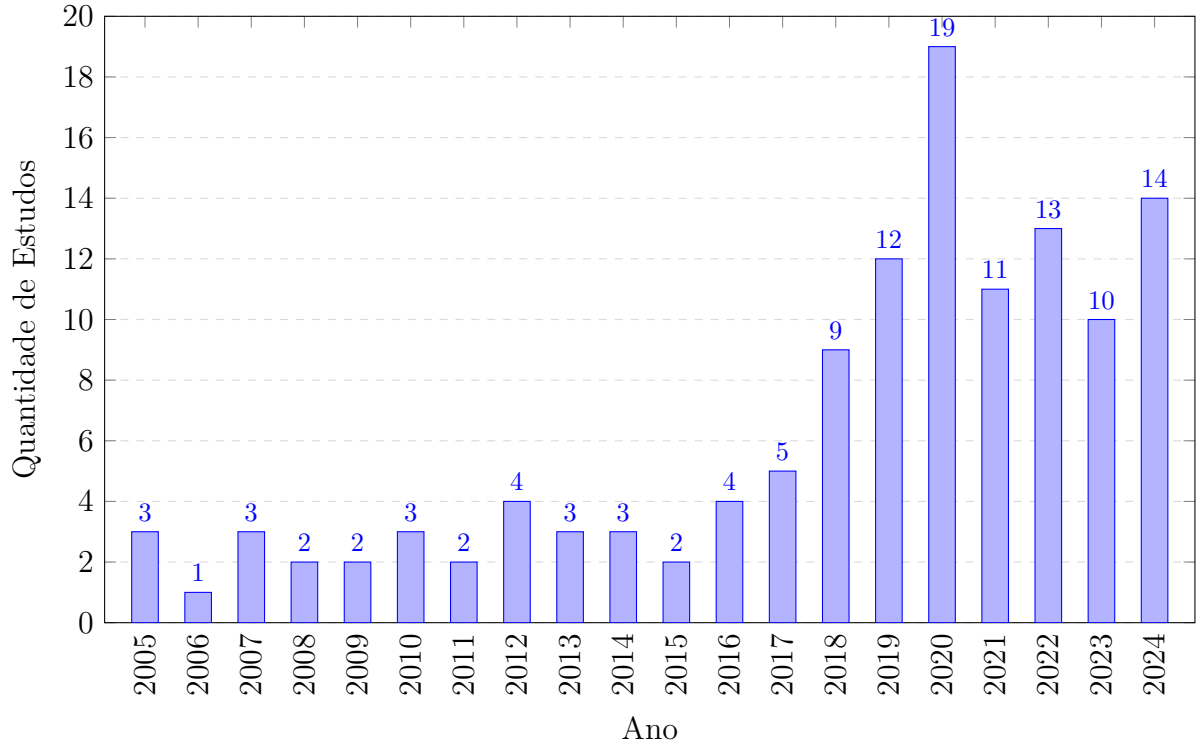

Figura 3.3: Distribuição dos Estudos por Ano de Publicação

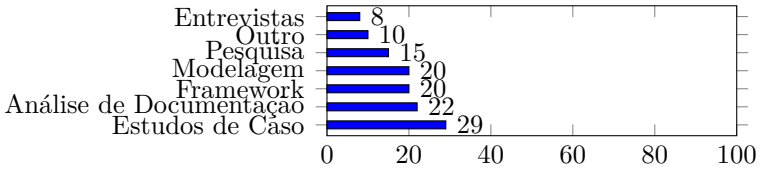

Figura 3.4: Número de estudos por Métodos

resultados impactariam nelas. Os estudos são: [42], [44], [48], [51], [53], [20], [21], [67], [69], [77], [79], [81], [86], [87], [96], [97], [98], [100], [106], [109], [111], [112], [113], [115], [23], [26], [118], [130], [121], [122], [126], [128], [101], [132], [135], [137], [140], [144], [147], [149].

Oitenta e oito (88) estudos primários foram conduzidos em contextos acadêmicos, nos quais os autores identificaram ou propuseram técnicas, métodos, processos, *frameworks* ou ferramentas e testaram suas propostas com estudantes ou em projetos hipotéticos. Por outro lado, 33 estudos foram realizados em um contexto industrial, onde os autores validaram suas propostas utilizando projetos reais da indústria de software. Além disso, 4 estudos consistiram exclusivamente em revisões de literatura sobre as técnicas utilizadas, ilustrando suas aplicações, conforme mostrado na Figura 3.5.

Trinta e quatro (34) estudos identificaram relações entre diferentes requisitos de privacidade. Por exemplo, Tsohou et al. [93] afirmam que os requisitos de privacidade devem

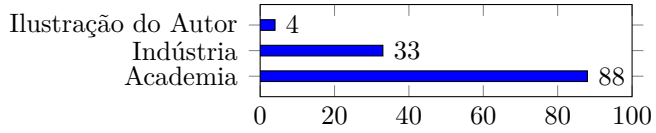

Figura 3.5: Distribuição dos estudos primários baseados no contexto de pesquisa

estar alinhados com segurança, leis e critérios de aceitação, abordando aspectos como privacy by design, gestão de consentimento e avaliações de impacto à privacidade, ao mesmo tempo em que garantem conformidade com as obrigações da GDPR. Herwanto et al. [101] identificam a privacidade como um dos seis requisitos fundamentais para sistemas IoT, observando que os requisitos de privacidade estão interligados a contextos como autenticação, confidencialidade e controle de acesso.

Além disso, quinze (15) estudos enfatizaram os impactos positivos dos requisitos de privacidade na Engenharia de Requisitos (ER), seis (6) mencionaram impactos negativos e cinquenta e seis (56) estudos destacaram tanto impactos negativos quanto positivos.

No geral, os estudos primários enfatizaram que os impactos positivos dos requisitos de privacidade na Engenharia de Requisitos (ER) incluem o aprimoramento do entendimento e da satisfação das necessidades dos *stakeholders*, o suporte à tomada de decisões organizacionais [51], a orientação do desenvolvimento de software e a gestão da conformidade regulatória.

Ao integrar a privacidade desde os estágios iniciais, é possível prevenir violações de direitos, aumentar a confiança do usuário e garantir maior transparência no uso de dados. Além disso, a conformidade legal com regulamentações como a GDPR e a LGPD é assegurada [59], resultando em um desenvolvimento de sistemas mais seguro e voltado para a proteção da privacidade dos dados do usuário.

Quanto aos aspectos negativos, os estudos destacam desafios relacionados à complexidade e à falta de clareza na implementação de leis como a GDPR, incluindo terminologias ambíguas e dificuldades na tradução dos princípios legais em requisitos de privacidade [49]. Outro problema crítico é o conflito entre requisitos de privacidade e outras demandas, como controle de identidade, especialmente em ambientes IoT [115].

Além disso, a imutabilidade de tecnologias como o *blockchain* pode dificultar o cumprimento das leis de privacidade de dados, que exigem a possibilidade de exclusão de informações pessoais. Estudos também indicam que o gerenciamento inadequado de requisitos de privacidade pode resultar em softwares de baixa qualidade e aumentar os riscos de sanções legais [132].

3.8.1 RQ.1 e RQ.2. Técnicas, métodos, processos, *frameworks* e ferramentas

Os estudos selecionados nesta RSL apresentaram diversas técnicas, métodos, processos, *frameworks* e ferramentas, tanto propostas quanto aplicadas na literatura, em diferentes estágios da Engenharia de Requisitos. No entanto, a maioria dos estudos adotou abordagens já existentes. A Tabela 3.5 apresenta os estudos analisados e os respectivos métodos utilizados em cada um.

Nome	Tipo	Referências
Security quality requirements engineering (SQUARE)	Processo	[43], [53], [69], [76], [78], [79], [102], [114]
Secure Tropos	Método	[39], [40], [46], [49], [54], [55], [69], [70], [71], [96], [99], [102], [104], [109], [110], [19], [114], [115], [137]
PriS	Método	[39], [40], [44], [46], [48], [49], [52], [55], [20], [69], [70], [75], [76], [79], [82], [85], [95], [96], [102], [106], [108], [114], [117]
i* (i-star)	Framework	[37], [39], [46], [49], [55], [79], [96], [104], [109], [114]
LINDDUN	Método	[37], [38], [49], [52], [22], [69], [102], [108], [114], [144], [146]
STRuctured Analysis for Privacy (STRAP)	Framework	[44], [46], [49], [55], [57], [96], [105], [114]
Privacy By Design (PbD)	Método	[38], [55], [59], [20], [61], [22], [68], [74], [86], [114], [143]

Tabela 3.5: Principais Técnicas, Métodos, Processos, Frameworks e Ferramentas utilizadas na Literatura

SQUARE O SQUARE (Security Quality Requirements Engineering), desenvolvido pelo programa de engenharia de software NSS (Networked Systems Survivability), foi criado para identificar e priorizar requisitos de privacidade em projetos de software. O processo SQUARE é composto pelos seguintes passos [43]: 1. Concordar sobre as definições; 2) Identificar Recursos e Metas de Privacidade; 3) Coleta de Artefatos; 4) Avaliação de Riscos; 5) Escolher a Técnica de Elicitação; 6) Elicitação dos Requisitos de Segurança; 7) Categorizar Requisitos; 8) Priorizar Requisitos; e 9) Inspecionar Requisitos. Embora o SQUARE tenha sido originalmente desenvolvido para requisitos de segurança, diversos estudos o adaptaram para atender às demandas de privacidade, como [53] e [76]. Além disso, [43] demonstrou como o processo pode ser ajustado para abordar preocupações relacionadas à privacidade, destacando as modificações específicas necessárias em cada etapa para melhor alinhamento com esses requisitos.

Secure Tropos O método Secure Tropos [99] é uma extensão da metodologia Tropos [154], desenvolvida para integrar questões de privacidade no desenvolvimento de sistemas orientados a agentes. Inicialmente concebida para modelar requisitos em sistemas multiagentes, a abordagem foi expandida para contemplar requisitos de privacidade desde os estágios iniciais da engenharia de requisitos até a sua finalização. Embora o método

Secure Tropos tenha sido originalmente focado em requisitos de segurança, ele pode ser adaptado para abranger requisitos de privacidade. Estudos como os de [99] e [71] avaliaram sua aplicabilidade na elicitação de requisitos de segurança e privacidade em um único cenário, sugerindo modificações para ampliar sua utilização em diferentes contextos. Além disso, [110] aplicou o método Secure Tropos para elicitar requisitos de privacidade e segurança com base em leis e regulamentações voltadas à proteção de dados.

PriS Method O método PriS é uma abordagem da engenharia de requisitos de segurança que integra requisitos de privacidade desde o início do processo de desenvolvimento de software [44]. Ele trata os requisitos de privacidade como metas organizacionais e propõe o uso de padrões do processo de privacidade para descrever os impactos desses requisitos e dos processos de negócios identificados no sistema de arquitetura, destacando como esses processos podem ser melhor apoiados pelas medidas de privacidade. O método PriS segue quatro atividades principais: 1) Elicitação de metas de privacidade; 2) Análise de impacto; 3) Modelagem de processos afetados; e 4) Identificação da implementação de técnicas.

i* (i-star) O *framework* i* (i-star ou i-estrela) é uma abordagem orientada a metas e atores [155]. Sua função primária é analisar e registrar as interações estratégicas entre agentes ou entidades responsáveis por ações em um sistema, juntamente com as motivações que levam a essas interações. O *framework* pode ser aplicado em diversos estágios do desenvolvimento de software, como elicitação e análise de requisitos, design de sistemas e análise organizacional. Alguns estudos, como [104], utilizam esse *framework* para apoiar e comparar os seus próprios *frameworks* e modelos desenvolvidos. No processo de avaliação do *framework* desenvolvido neste estudo, o i* foi um dos três *frameworks* utilizados para comparação.

LINDDUN A metodologia LINDDUN é um *framework* desenvolvido para analisar e abordar problemas de privacidade em sistemas, com foco primário na incorporação de privacidade desde os estágios iniciais do desenvolvimento de software. Essa abordagem facilita a identificação de potenciais ameaças à segurança [37]. LINDDUN é baseada na decomposição das ameaças de privacidade em sete categorias principais: 1) Linkabilidade: foca na habilidade de relacionar duas ou mais atividades ou atributos a um único; 2) Identificabilidade: refere-se à habilidade de identificar um indivíduo dentro de um conjunto de dados; 3) Não repúdio: garante que um indivíduo não possa negar ter realizado uma ação; 4) Detectabilidade: envolve a habilidade de um ataque para detectar qual informação específica se encontra em um conjunto de dados; 5) Divulgação de Informações: relacionada ao vazamento de informações pessoais, mesmo quando não diretamente

associadas a um indivíduo; 6) Inconsciência: aborda a falta de conscientização de um indivíduo sobre como seus dados estão sendo utilizados; 7) Não-Conformidade: falha em aderir às leis e regulamentações de privacidade. É importante notar que esta metodologia apresenta uma taxonomia detalhada de ameaças à privacidade e seus impactos, sugere técnicas de mitigação adaptadas ao cenário de desenvolvimento de sistemas e identifica riscos. Alguns estudos utilizam a metodologia LINDDUN como base e referência, como demonstrado pelo estudo de [22]. Esse estudo identifica 56 ameaças à privacidade, categorizadas com o *framework* LINDDUN, e apresenta recomendações para mecanismos de mitigação apropriados para cada uma das ameaças identificadas.

STRuctured Analysis for Privacy (STRAP) O *framework* STRAP [105] é uma abordagem leve e estruturada para analisar vulnerabilidades de privacidade no design de sistemas. Este *framework* utiliza uma análise orientada a metas para identificar vulnerabilidades à privacidade, categorizá-las e propor soluções ou estratégias para mitigá-las. O *framework* STRAP consiste em quatro passos: 1) Análise: atores do sistema, metas e componentes são identificados, e um conjunto de questões analíticas é aplicado a cada meta e sub-meta; 2) Refinamento: após as vulnerabilidades serem identificadas, o próximo passo é decidir como eliminá-las ou mitigá-las, dependendo do contexto; 3) Avaliação: diferentes designs ou soluções são comparados com base na sua efetividade em reduzir os riscos de privacidade; e 4) Iteração: o *framework* suporta um processo iterativo, permitindo uma reavaliação do sistema para ajustar mudanças ou novas funcionalidades quando elas são criadas.

Privacy By Design (PbD) Privacy by Design (PbD) [156] é um método que integra a privacidade como um princípio fundamental no design e desenvolvimento de sistemas, processos e produtos. PbD foca em garantir que a privacidade seja considerada desde o início e durante todo o ciclo de vida do projeto, em vez de tratá-la como uma preocupação secundária ou algo a ser pensado posteriormente. PbD foi construído em sete princípios fundamentais [156]: 1) Proativo, não reativo; preventivo, não corretivo; 2) Privacidade como configuração padrão; 3) Privacidade inserida no design; 4) Funcionalidade total: soma positiva, não soma zero; 5) Segurança de ponta a ponta: ciclo de vida de proteção total; 6) Visibilidade e transparência: manter em aberto; e 7) Respeito pela privacidade do usuário: manter centrado no usuário. Neste contexto, [114] analisou metodologias de privacidade existentes, examinando como LINDDUN, SQUARE e PriS se alinhavam com o *framework* de Privacy By Design. O estudo avaliou a conformidade desses *frameworks* e seus suportes aos princípios de PbD. Os resultados mostraram resultados satisfatórios

para a avaliação das metodologias, confirmando a conformidade com os padrões de PbD e suas capacidades de suportar PbD.

Técnicas Adicionais Propostas Além das técnicas, métodos, processos, *frameworks* e ferramentas anteriormente apresentadas, outros estudos utilizam um ou mais técnicas, como podemos ver na Tabela 3.6 eles são: **1) KAOS method** ([46], [49], [55], [69], [96], [102], [109]); **2) Goal-Based Requirements Analysis Method (GBRAM)** ([42], [46], [49], [55], [96], [112]); **3) Role-Based Access Control (RBAC)** ([46], [49], [55], [66], [114]); **4) STRIDE** ([37], [22]); **5) PRIPARE** ([22], [77]); **6) P-STORE** ([77], [80]); **7) ISO 29100** ([59], [68], [107], [112]); **8) Bellotti-Sellen Framework** ([46], [96], [105]); **9) Moffett-Nuseibeh Framework (M-N)** ([46], [55], [96]); **10) SecTro** ([54], [71], [79], [128]); **11) Privacy Criteria Method (PCM)** ([69], [81], [82], [126]); **12) ConfIS** ([54], [128]); **13) SepTA** ([79], [128]); **14) Privacy Impact Assessment (PIA)** ([38], [77], [92], [119], [149]); **15) Asia-Pacific Economic Cooperation (APEC) Privacy Framework** ([42], [47], [119]); **16) Non-Functional Requirement Framework (NFR)** ([46], [49], [55], [64], [69], [104], [122], [60]); **17) OECD Privacy Statement Generator** ([53], [76]); and **18) NIST** ([58], [119], [121]).

[109] apresenta um catálogo de conceitos relacionados à privacidade, que inclui i* (I-star), Tropos, Quadro de Problemas, NFR Framework, SI* Framework, GRL, Modelo de Ameaças, uso de mapas de caso, SecBPMN-ml, UML4PF, Diagramas de Fluxo de Dados, KAOS, Modelagem Orientada a Agente/Metas, Secure Tropos, Casos de Mau Uso, UMLsec, UML, STS-ml, Legal GRL, CORAS Risk Modeling, Anotação de Requisitos de Usuário, BPMN, Security-Aware Tropos e Árvore de Ameaças. Por fim, é importante notar que muitos dos estudos primários identificados na RSL propõem um *framework* ou modelo que pode servir como uma ferramenta nos estágios de engenharia de requisitos para tratar requisitos de privacidade, como mostrado na Tabela 3.7.

RQ.1 e RQ.2 Sumário: De acordo com a literatura, as técnicas, métodos, processos *frameworks* e ferramentas mais utilizadas são: SQUARE, Secure Tropos, PriS, I* (I-Star), LINDDUN, STRAP e Privacy by Design.

3.8.2 RQ.3 Técnicas, métodos, processos, frameworks e ferramentas utilizadas em cada fase da ER

Dos 125 estudos primários selecionados, 4 focaram em especificar os estágios da Engenharia de Requisitos, como mostrado na Figura 3.6. A maioria dos estudos concentrou-se na fase de elicitação de requisitos e propôs *frameworks* ou modelos para abordar os requisitos

KAOS method	[46], [49], [55], [69], [96], [102], [109]
Goal-Based Requirements Analysis Method (GBRAM)	[42], [46], [49], [55], [96], [112]
Role-Based Access Control (RBAC)	[46], [49], [55], [66], [114]
STRIDE	[37], [22]
PRIPARE	[22], [77]
P-STORE	[77], [80]
ISO 29100	[59], [68], [107], [112]
Bellotti-Sellen Framework	[46], [96], [105]
M-N (Moffett-Nuseibeh Framework)	[46], [55], [96]
SecTro	[54], [71], [79], [128]
PCM (Privacy Criteria Method)	[69], [81], [82], [126]
ConfIS	[54], [128]
SepTA	[79], [128]
Privacy Impact Assessment (PIA)	[38], [77], [92], [119], [149]
Asia-Pacific Economic Cooperation (APEC) Privacy Framework	[42], [47], [119]
Non-Functional Requirement Framework (NFR)	[46], [49], [55], [64], [69], [104], [122], [60]
OECD Privacy Statement Generator	[53], [76]
NIST	[58], [119], [121]

Tabela 3.6: Métodos Adicionais Propostos

de privacidade. A Tabela 3.8 apresenta todos os estudos juntamente com as respectivas fases da Engenharia de Requisitos que eles abordam.

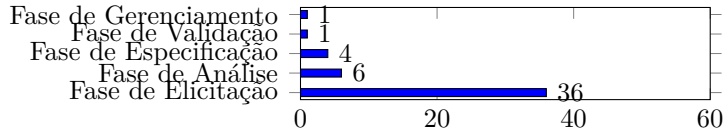

Figura 3.6: Número de estudos por fase de Engenharia de Requisitos

[87] introduz uma ferramenta de gerenciamento de requisitos para Sistemas Ciberfísicos (CPS), com o objetivo de aumentar o controle e a transparência do usuário ao gerenciar requisitos de privacidade. Essa ferramenta permite a execução automatizada de

Framework/Modelo	Referências
Requisitos de privacidade em IoT	[35] [35], [64]
Conceitos de privacidade	[36], [38], [50], [79]
Ameaça à privacidade e análise de requisitos	[37], [54], [65], [72], [79], [92], [111], [116], [148]
Elicitação de requisitos de privacidade	[39], [40], [42], [53], [58], [59], [63], [68], [69], [70], [77], [78], [81], [82], [83] [84], [87], [89], [96], [104], [106], [108], [110], [132], [137], [139], [141], [143], [145], [146], [150], [152]
Requisitos de privacidade para brinquedos inteligentes	[41]
Alinhamento de requisitos de segurança e privacidade	[46], [51], [52], [113], [144], [149], [151]
PriS	[44], [48], [20], [75], [85], [117]
COPri	[56], [57]
Privacy By Design, RBAC, PRET, P-STORE, Privacy-Enhanced BPMN (PE-BPMN), EPICUREAN, Secure Tropos, STRAP, TrUStAPIS	[61], [66], [76], [80], [91], [97], [99], [105], [115]
Conformidade com requisitos de privacidade	[95], [107], [112], [133], [136], [137], [138], [142], [143], [147]
Requisitos de privacidade em BlockChain	[98]
Requisitos de privacidade no Metaverso	[103]

Tabela 3.7: Frameworks/Modelos Encontrados

Fase da ER	Referência
Elicitação	[20], [75], [117], [44], [53], [76], [36], [46], [48], [70], [55], [90], [102], [106], [51], [21], [74], [49], [88], [92], [97], [113], [56], [109], [115], [54], [57], [80], [69], [42], [47], [59], [77], [100], [112], [151]
Análise	[105], [96], [67], [111], [79], [91]
Especificação	[86], [95], [22], [81]
Validação	[43]
Gerenciamento	[87]

Tabela 3.8: Estudos relacionados às fases da Engenharia de Requisitos

modelos comportamentais e valida o comportamento do modelo durante o tempo de execução. Isso facilita o gerenciamento de privacidade, promovendo autonomia transparente e compartilhada entre os componentes de CPS.

Os estudos [56] e [57] apresentam o desenvolvimento das ontologias COPri e COPri v.2, que visam auxiliar na fase de elicitação de requisitos de privacidade. Esses estudos concentram-se na criação e no refinamento de uma ontologia que aborda um problema comum enfrentado pelos engenheiros de requisitos: a falta de entendimento sobre as necessidades específicas de privacidade, diferenciando-as de outros tipos de requisitos, como segurança. A ontologia oferece um conjunto de conceitos-chave compreensíveis e expressivos, além de relações vinculadas à privacidade, incluindo o consentimento dos titulares de dados, avaliação de riscos e gerenciamento de ameaças à privacidade, como anonimização e minimização de dados.

[43] utilizou o processo SQUARE para validar os requisitos de privacidade necessários para uma aplicação de software. [37] e [22] empregaram o *framework* LINDDUN para

especificar requisitos de privacidade e identificar potenciais riscos à privacidade, categorizados nas sete categorias de LINDDUN, facilitando assim o processo de especificação dos requisitos de privacidade.

[79] propôs uma ferramenta para modelar e analisar requisitos, incluindo requisitos de privacidade, segurança e confiança, focando em minimizar os esforços dos desenvolvedores de software para entender esses requisitos.

[21] introduziu o conceito de "*Early Privacy*", enfatizando a importância de considerar a privacidade como valor fundamental durante todas as fases do ciclo de vida do desenvolvimento de software. Os autores criaram questionários, personas, cenários e protótipos de design participativo para elicitar requisitos de privacidade dentro de sistemas de computação ubíqua, garantindo que os requisitos de privacidade estivessem alinhados com os modelos mentais dos usuários.

RQ.3 Sumário: A maioria dos estudos utilizou técnicas, métodos, processos, *frameworks* e ferramentas durante a fase de elicitação de requisitos, enquanto alguns estudos focaram no gerenciamento, validação e estágios de especificação.

3.8.3 RQ.4 Desafios na Elicitação de Requisitos de Privacidade

A maioria dos estudos selecionados nas fases da RSL apontou dificuldades/desafios na elicitação de requisitos de privacidade. No entanto, um padrão surgiu nos problemas mencionados, especialmente nas práticas de implementação de requisitos de privacidade. Os principais problemas e desafios identificados foram: 1) o aumento da complexidade no desenvolvimento de software, particularmente durante a fase de engenharia de requisitos, e 2) um conflito direto com requisitos de segurança, em que, em alguns casos, os membros das equipes não conseguiam distinguir claramente os requisitos de segurança dos requisitos de privacidade.

Aumento na Complexidade de Desenvolvimento de Software

A maioria dos estudos indica que os principais desafios na elicitação de requisitos de privacidade durante a fase de engenharia de requisitos estão relacionados ao aumento da complexidade das atividades envolvidas nesse estágio. Essa complexidade decorre de vários fatores, como a dificuldade que analistas/engenheiros de requisitos e *stakeholders* têm em entender os requisitos de privacidade e em aplicá-los na prática, bem como os desafios em compreender as regulamentações e padrões existentes de privacidade de dados.

[42], [36], [38], [70], [83] e [100] mencionam que um dos fatores que contribuem para o aumento da complexidade no desenvolvimento de software está relacionado à dificuldade

de entendimento e conhecimento dos requisitos de privacidade. Os autores enfatizam que há um fardo adicional de conhecimento sobre as leis de privacidade para os desenvolvedores ao lidar com esses requisitos. Além disso, notaram que há frequentemente um baixo engajamento dos membros das equipes ao tratar de problemas relacionados aos requisitos de privacidade, tanto pela complexidade desses requisitos quanto pela falta de ferramentas adequadas para gerenciá-los.

[45] e [77] também destacaram que a elicitação de requisitos de privacidade pode comprometer a agilidade no processo de desenvolvimento. Canedo *et al.* [45] investigou os desafios enfrentados por equipes ágeis ao abordar requisitos de privacidade e sugeriu que as equipes de desenvolvimento utilizem *checklists* com uma linguagem mais simples para discutir e apresentar requisitos de privacidade aos *stakeholders*. Essa abordagem pode ajudar a reduzir o impacto negativo na agilidade da equipe. Além disso, em [77] existe uma recomendação que equipes ágeis utilizem ferramentas automatizadas para revisar requisitos de privacidade.

[53] enfatiza a necessidade de uma metodologia eficiente durante a fase de Engenharia de Requisitos (ER) para abordar requisitos de privacidade, destacando que gerenciar esses requisitos é complexo devido à restrição de tempo nas atividades de ER. Esse processo também exige que os praticantes reconheçam as leis de privacidade e as técnicas necessárias para garantir a privacidade. Da mesma forma, em [55] e [112] são reportadas as dificuldades dos praticantes em lidar com os conceitos complexos presentes nas legislações e políticas de privacidade. Além disso, [68] explorou como requisitos de privacidade podem ser vagos e desconexos da tecnologia, aumentando a complexidade e os desafios para a implementação desses requisitos na prática.

Dadas as várias abordagens disponíveis para lidar com os requisitos de privacidade, [67] discute a importância de selecionar estratégias apropriadas para gerenciar os requisitos de privacidade em diferentes contextos. Os autores enfatizaram a necessidade de escolher cuidadosamente entre abordagens como "privacy-by-policy"e "privacy-by-architecture". Escolher a prática de privacidade errada pode levar a custos adicionais de desenvolvimento e complexidades desnecessárias. [107] também apresenta o desafio de escolher a melhor abordagem para gerenciar requisitos de privacidade, sugerindo que os *stakeholders* analisem cuidadosamente os prós e contras de diferentes estratégias de privacidade de dados apresentadas pelos times de desenvolvimento de software.

[62] e [47] recomendam que as equipes de desenvolvimento explorem a possibilidade de automatizar o processo de elicitação de requisitos aplicando técnicas de Processamento de Linguagem Natural (PLN). Essa abordagem pode ajudar a identificar não apenas requisitos de privacidade, mas também requisitos de segurança. Além disso, [90] sugeriu o desenvolvimento de novos modelos de requisitos de privacidade, enfatizando a neces-

sidade de uma perspectiva mais aprofundada sobre privacidade, considerando conceitos complexos como privacidade de localização e atributos derivados probabilisticamente.

Requisitos de Privacidade vs. Requisitos de Segurança

[37], [39], [40], [46], [57], [113], e [113] reportaram dificuldades na integração de requisitos de privacidade e segurança. Embora ambos se concentrem primariamente na proteção de dados, os conceitos fundamentais frequentemente divergem e, por vezes, entram em conflito durante a fase de Engenharia de Requisitos. Enquanto a maioria dos estudos apenas destaca esses desafios e sugere pesquisas futuras para resolver esses conflitos, alguns, como em [46] e [113], propuseram abordagens para mitigar e resolver os conflitos entre requisitos de privacidade e segurança.

[113] destaca os desafios e conflitos entre requisitos de privacidade e segurança, com foco particular em requisitos de Anonimização e Inobservância (requisitos de privacidade que permitem que entidades usem recursos sem revelar suas identidades). Os autores observaram que esses requisitos frequentemente entravam em conflito com requisitos de segurança, como Responsabilização e Auditabilidade (que exigem o rastreamento de atividades e a vinculação das ações a entidades específicas). Para abordar esses e outros conflitos, os autores propuseram a identificação de ferramentas capazes de apoiar simultaneamente os requisitos de privacidade e segurança. Eles enfatizaram a importância de avaliar essas ferramentas em diferentes contextos para otimizar seu uso e desempenho.

Em [46] é enfatizada a necessidade de um *framework* automatizado para apoiar as equipes de desenvolvimento de privacidade na modelagem das relações entre requisitos de privacidade e segurança. Eles apresentaram o desenvolvimento inicial de um *framework* projetado para ajudar os desenvolvedores a elicitar questões de privacidade e segurança nas fases iniciais do processo de desenvolvimento.

Outros Desafios

Alguns estudos mencionaram desafios em contextos específicos que, embora não representem um problema generalizado, como o aumento da complexidade nas fases de Engenharia de Requisitos e Desenvolvimento de Software, apresentam problemas significativos em suas respectivas áreas de conhecimento. [35] apresenta os desafios de lidar com requisitos de privacidade em contextos de IoT, enfatizando que os serviços nesse domínio dependem fortemente da coleta de dados para funcionar corretamente. O estudo propôs uma possível solução para mitigar esse problema, sugerindo que os desenvolvedores aproveitem os dados existentes ou as percepções provenientes de pesquisas auto-coletadas para informar o design das interfaces de configuração de privacidade. Essa abordagem demonstra a ne-

cessidade de um processo de design cuidadoso para abordar efetivamente as preocupações com requisitos de privacidade.

Huth *et al.* [49] enfatizou a necessidade de modelos conceituais para auxiliar no entendimento dos conceitos de privacidade apresentados na General Data Protection Regulation (GDPR) [5], observando que a definição de privacidade na legislação contribui para confusão sobre as medidas que devem ser tomadas para garantir a privacidade dos dados do usuário. Da mesma forma, [108] destaca os desafios na interpretação dos princípios da GDPR, que podem levar a ambiguidades sobre como os requisitos de privacidade podem ser integrados nos requisitos de engenharia, potencialmente resultando em problemas relacionados à conformidade com a lei. Como solução parcial para esse problema, [88] apresentou 13 padrões de controle de privacidade que oferecem soluções orientadas a problemas e baseadas em padrões para os requisitos técnicos da GDPR. O estudo [93] identificou e consolidou 393 requisitos englobando aspectos legais de privacidade, segurança e aceitação de tecnologia.

RQ.4 Sumário: Os principais desafios em abordar requisitos de privacidade incluem o aumento da complexidade no desenvolvimento de software, particularmente durante a fase de engenharia de requisitos, e conflitos diretos entre requisitos de privacidade e segurança. Esses conflitos regularmente levam a uma confusão entre os membros das equipes, dificultando a distinção entre os dois tipos de requisitos.

Capítulo 4

Análise e Discussão dos Resultados

4.1 Questionário de pesquisa

Também foi conduzida uma pesquisa para entender se as técnicas, métodos, processos, *frameworks* e ferramentas de Engenharia de Requisitos (ER) comumente descritos na literatura para elicitação, análise, especificação, validação e gerenciamento de requisitos de privacidade são conhecidas ou utilizadas pelos profissionais. A plataforma do Google Forms foi utilizada para criar o questionário da pesquisa.

Antes da aplicação definitiva, foi realizada uma rodada piloto para avaliar a qualidade do questionário. Três profissionais da área de privacidade participaram desse teste, fornecendo *feedback* sobre a linguagem utilizada nas questões, a remoção de perguntas redundantes, ajustes em intervalos de tempo e a inclusão/modificação de algumas opções de resposta. As sugestões foram implementadas, resultando em melhorias na pesquisa. Os entrevistados do piloto levaram cerca de 10 minutos para completar o questionário, informação que foi incluída na versão final disponibilizada ao público.

A pesquisa consistiu em 16 perguntas: 15 de múltipla escolha e 1 aberta. No início do questionário, foi apresentado um termo de consentimento contendo os termos e condições da pesquisa. A participação foi anônima, e nenhuma informação de contato foi solicitada aos respondentes. O questionário foi divulgado em diversas plataformas, incluindo LinkedIn, Facebook e Instagram, e permaneceu aberto de 1º a 28 de novembro de 2024, totalizando 28 dias.

Ao todo, 31 profissionais responderam à pesquisa. A maioria dos participantes é da região Centro-Oeste (28 respondentes) e possui mais de quatro anos de experiência em desenvolvimento de software (21 respondentes), atuando principalmente como programadores/desenvolvedores. A Tabela 4.1 apresenta o perfil detalhado dos participantes.

Setenta e um por cento (71%) dos participantes declararam que já trabalharam ou trabalham atualmente no desenvolvimento de funcionalidades de software que envolvem

Região	#	%
Sudeste	1	3.2
Centro-Oeste	29	93.5
Sul	1	3.2
Idade	#	%
21 a 25 anos	10	32.3
26 a 30 anos	4	12.9
31 a 36 anos	2	6.5
37 a 42 anos	5	16.1
43 a 47 anos	6	19.4
48 a 54 anos	4	12.9
Nível Educacional	#	%
Estudante de Graduação	6	19.4
Graduação	3	9.7
Especialização	2	6.5
Estudante de Mestrado	12	38.7
Mestrado	2	6.5
Estudante de Doutorado	4	12.9
Doutorado	2	6.5
Experiência	#	%
>=1 ano	4	12.9
Entre 1 e 3 anos	4	12.9
Entre 4 e 6 anos	7	22.6
Entre 7 e 10 anos	2	6.5
Entre 11 e 15 anos	3	9.7
Entre 16 e 20 anos	6	19.4
Mais de 21 anos	5	16.1
Organização	#	%
Administração Pública Federal	13	41.9
Administração Pública Estadual	6	19.4
Empresa Privada de Desenvolvimento de Software	9	29
Projetos de colaboração/pesquisa	3	9.7
Cargo	#	%
Programador/Desenvolvedor de Software	23	74.2
Engenheiro de Requisitos	3	9.6
Gestor de Segurança da Informação	5	16.2

Tabela 4.1: Perfil demográfico dos participantes da pesquisa (n= 31).

preocupações com a privacidade de dados. No entanto, 29% relataram que não (Q7).

Além disso, 87% dos participantes "concordam totalmente"ou "concordam"que suas organizações implementaram ou estão em processo de implementação de mudanças devido à Lei Geral de Proteção de Dados (LGPD) (Q8).

No que diz respeito ao conhecimento sobre a LGPD, 71% afirmaram que possuem conhecimento suficiente para desenvolver suas atividades nos projetos em que estão envolvidos. No entanto, 19,4% declararam que não possuem o conhecimento necessário para

implementar a LGPD (Q9) (Imagem 4.1).

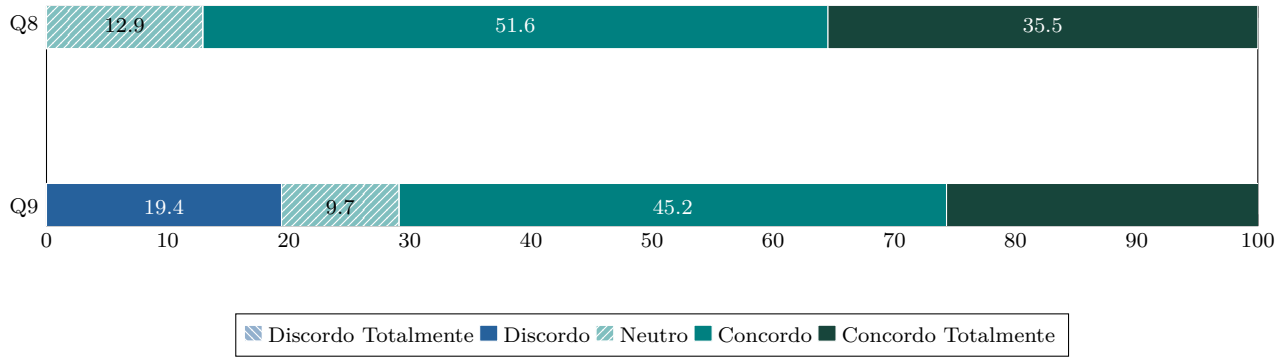

Figura 4.1: Percepção dos Profissionais

Também foram investigados quais princípios da LGPD eram familiares para os participantes (Q10). Os princípios mais conhecidos foram segurança, qualidade dos dados, transparência e finalidade, conforme ilustrado na Imagem 4.2. Esse resultado é semelhante ao identificado por [4] e [3], em que os participantes desses estudos também demonstraram maior familiaridade com esses princípios.

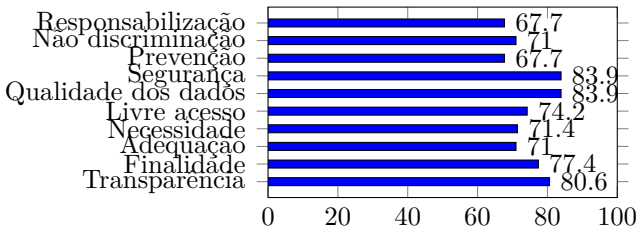

Figura 4.2: Princípios da LGPD conhecidos pelos profissionais

Em relação aos princípios da LGPD que as organizações dos participantes utilizam ou implementam (Q11), os profissionais relataram que os mais comuns são Segurança (83,9%), Finalidade (71%), Qualidade dos Dados (71%) e Transparência (64,5%). Esse achado está alinhado com [4], que também identificou os princípios de segurança e finalidade como os mais implementados pelos profissionais.

Sobre as técnicas, métodos, processos, frameworks e ferramentas com as quais os profissionais já trabalharam ou ainda trabalham (Q12), apenas oito participantes relataram ter experiência com Privacy by Design (PbD), e, entre eles, apenas alguns mencionaram o uso da ISO 29100 e SQUARE. A maioria dos profissionais ainda não utilizou técnicas identificadas na literatura. Esse resultado diverge de [3], onde muitos participantes relataram utilizar Pris, NFR, RBAC, PbD, PCM e PET.

Quanto à fase da Engenharia de Requisitos em que os profissionais aplicaram técnicas, métodos, processos, frameworks e ferramentas para tratar requisitos de privacidade (Q13),

a maioria relatou que isso ocorreu principalmente na fase de análise de requisitos (61,3%) e na fase de especificação (48,8%), conforme ilustrado na Imagem 4.3.

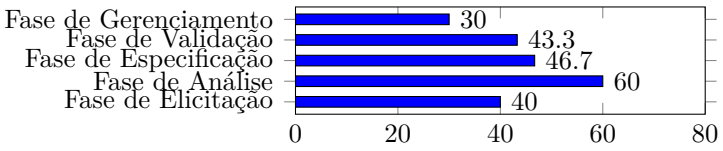

Figura 4.3: Técnicas por fase de Engenharia de Requisitos

Sobre as ferramentas utilizadas pelos times de desenvolvimento de software para elicitar e documentar requisitos de privacidade (Q14), a maioria dos participantes relatou não utilizar nenhuma ferramenta específica. No entanto, 4 participantes declararam ter utilizado o SMaRT, e 2 participantes mencionaram o uso de PRIS, Strap e SPARQL, respectivamente. Essas descobertas são semelhantes às observações de [157].

Quanto aos desafios enfrentados pelos profissionais na elicitação de requisitos de privacidade, um dos participantes, identificado como #P19, afirmou: "As leis de privacidade podem mudar, e é necessário que os requisitos de privacidade estejam sempre alinhados com as regulamentações mais recentes. Além disso, em sistemas sensíveis ao contexto, como os de IoT, a coleta e o uso de dados aumentam a necessidade de requisitos de privacidade específicos, pois esses sistemas frequentemente lidam com informações pessoais sensíveis."

4.2 Discussões

A maioria dos estudos selecionados na RSL focou na fase de elicitação de requisitos, destacando várias técnicas, métodos, processos, *frameworks* e ferramentas utilizadas na literatura para abordar requisitos de privacidade. O uso predominante de *frameworks* como SQUARE, Secure Tropos, PriS, I-Star, LINDDUN, STRAP e PbD demonstra a necessidade de expandir recursos automatizados que ajudem engenheiros de requisitos a traduzir conceitos complexos de privacidade em práticas aplicáveis durante o desenvolvimento de software.

A ênfase dos estudos na fase de elicitação de requisitos sugere que as organizações devem investir em ferramentas automatizadas para apoiar atividades neste estágio, onde os *stakeholders* e analistas/engenheiros de requisitos frequentemente se equivocam sobre os requisitos de privacidade. No entanto, os esforços não devem se limitar apenas à atividade de elicitação de requisitos; devem ser estendidos para análise, documentação, validação e gerenciamento de requisitos durante todo o ciclo de desenvolvimento. Isso se torna ainda

mais crucial ao observar que alguns estudos abordaram as fases finais da Engenharia de Requisitos, destacando uma lacuna que deve ser explorada em futuras pesquisas.

Os estudos identificaram desafios na elicitação dos requisitos de privacidade, incluindo o aumento da complexidade no desenvolvimento de software e os requisitos de segurança e privacidade. Esses desafios indicam a necessidade de integrar abordagens já existentes. A complexidade surge da natureza intrínseca dos requisitos de privacidade e da necessidade de cumprir as leis de privacidade de dados, como a GDPR e a LGPD. A confusão entre esses requisitos pode levar a consequências como o não cumprimento da legislação e a insatisfação dos usuários, que esperam que suas informações pessoais sejam tratadas adequadamente.

As soluções propostas na literatura incluem *checklists* simplificadas e automação com NLP, que fornecem caminhos viáveis para mitigar esses desafios. Implementar essas estratégias pode facilitar as atividades nas fases de Engenharia de Requisitos e aumentar o conhecimento e engajamento entre os membros das equipes de desenvolvimento de software, especialmente os profissionais responsáveis por lidar com questões de privacidade. Isso cria uma cultura de responsabilidade que se estende por todas as fases do desenvolvimento. No entanto, uma pesquisa futura deve explorar a aplicação de novas ferramentas e *frameworks* que integrem efetivamente a privacidade no desenvolvimento de software. Também é essencial promover uma maior colaboração entre pesquisadores, desenvolvedores e reguladores para criar um entendimento conjunto das melhores práticas no gerenciamento da privacidade, contribuindo para um ecossistema de desenvolvimento de software que respeite e proteja os direitos do usuário.

Os resultados da pesquisa indicam que a maioria dos participantes tem experiência trabalhando em projetos de software envolvendo preocupações com a privacidade de dados e reconhece que suas organizações estão se adaptando à LGPD, embora ainda existam lacunas significativas no conhecimento e na implementação. Os participantes demonstram familiaridade relativamente alta com os princípios da LGPD, como segurança, finalidade e transparência, o que coincide com a literatura existente. No entanto, a aplicação prática de técnicas, métodos, processos, *frameworks* e ferramentas focados na privacidade ainda é limitada. O uso predominante de práticas informais ou a falta de ferramentas durante a elicitação de requisitos de privacidade revela uma necessidade urgente de um melhor entendimento e adoção de métodos estruturados por PbD. Essas descobertas oferecem uma oportunidade clara para oferecer treinamento direcionado e promover melhores práticas, conectando a lacuna entre o entendimento teórico e a implementação prática em engenharia de privacidade.

4.3 Ameaças à Validação

As ameaças à validação deste estudo podem ser categorizadas em quatro tipos principais: construto, interno, externo e conclusão [34]. Sobre a validade de construto, a preocupação primária está na ambiguidade potencial de definições para termos como "requisitos de privacidade"e "ferramentas", que podem variar dentre os estudos. Além disso, existe um risco de que os critérios de inclusão e exclusão possam não reunir todos os estudos relevantes. Para tratar desses riscos, definições claras de critérios de aceitação e exclusão foram estabelecidas, e revisão por pares foi conduzida para garantir a consistência na aplicação desses critérios.

Sobre a validação interna, uma ameaça comum foi observada em todas as Revisões Sistemáticas de Literatura, o risco de viés na seleção dos estudos, que pode levar a um julgamento subjetivo dos pesquisadores durante o processo de extração. Seguindo o guia estabelecido por Kitchenham et al. [32], foi possível implementar uma série de práticas para minimizar essa ameaça. Uma prática foi selecionar bases de dados recomendadas pelo guia para buscar os estudos. Além disso, aplicar um critério de qualidade rigoroso também contribuiu para mitigar os riscos mencionados acima, tanto para as bases de dados iniciais selecionadas quanto para as utilizadas na pesquisa manual conduzida após o primeiro estágio desta revisão.

Sobre a validação externa, a categorização das técnicas, métodos, processos, *frameworks* e ferramentas em subgrupos pode não capturar nuances entre abordagens ou sobrepor categorias, complicando a análise comparativa. Isso ocorre porque pequenas diferenças na metodologia ou aplicação podem levar a resultados divergentes entre ferramentas, mesmo quando são categorizadas e classificadas de maneira similar. Para lidar com esse problema, o critério de extração foi definido para garantir que diferentes nuances, contextos e detalhes possam ser extraídos de cada estudo analisado. Essa abordagem permite um nível de diferenciação entre estudos e ferramentas que tratam dos mesmos temas e contextos, aumentando a validação externa geral das descobertas, reconhecendo as complexidades e variações inerentes nos dados.

Sobre a validação da conclusão, a heterogeneidade dos estudos e a síntese qualitativa dos estudos pode introduzir uma subjetividade nas interpretações. Além disso, a evolução constante de regulamentações de privacidade e tecnologias pode afetar a relevância das descobertas com o tempo. Para mitigar as ameaças apresentadas neste contexto, um tempo limite de até 20 anos para aceitação dos estudos foi estabelecido, com ênfase maior na pesquisa dos últimos 10 anos. Essa abordagem foca em identificar técnicas da literatura que continuam relevantes e são utilizadas atualmente como referências fundamentais, enquanto ainda procura por metodologias inovadoras e atuais. Adicionalmente, uma classificação detalhada dos estudos foi realizada para entregar uma síntese dos seus

resultados, e uma revisão detalhada foi adotada para conduzir a Revisão Sistemática de Literatura.

Por fim, as principais ameaças à validação da pesquisa incluem: (1) Viés de amostragem, pois os participantes não representam totalmente a diversidade de organizações e níveis de maturidade de privacidade no Brasil; (2) Viés de auto-seleção, já que os profissionais mais familiarizados com a LGPD podem ter sido mais propensos a responder à pesquisa; e (3) Generalização limitada, pois o foco específico em privacidade pode restringir a aplicabilidade das descobertas a outros contextos organizacionais ou regionais.

Capítulo 5

Conclusão

Neste estudo, foram identificados 125 estudos primários que exploram várias técnicas, métodos, processos, *frameworks* e ferramentas empregadas na Engenharia de Requisitos para tratar requisitos de privacidade. Esta revisão destacou que, embora exista uma grande variedade de abordagens, a maioria das pesquisas está concentrada em contextos acadêmicos, com evidências limitadas de aplicação prática em larga escala em ambientes industriais. Abordagens amplamente utilizadas, como PriS Method, Secure Tropos, LINDDUN, i* (i-star), STRAP, Privacy by Design (PbD) e SQUARE, são focadas primariamente na fase de elicitação dos requisitos de privacidade, indicando uma ênfase significativa nos estágios iniciais da engenharia de requisitos. No entanto, a falta de pesquisas dedicadas aos estágios finais, como análise, documentação, validação e gerenciamento, aponta para uma necessidade urgente de uma futura exploração para garantir a integração compreensiva dos requisitos de privacidade durante todo o ciclo de desenvolvimento de software.

Adicionalmente, esta revisão identificou diversos desafios na elicitação de requisitos de privacidade, incluindo o aumento da complexidade no desenvolvimento de software e a confusão entre requisitos de segurança e privacidade. Esses desafios demonstram a necessidade de abordagens integradas que possam efetivamente lidar com as nuances da privacidade no contexto da evolução da regulamentação de proteção de dados. Os resultados do questionário destacam ainda mais esses desafios, revelando que muitos profissionais estão familiarizados com os princípios da LGPD e concordam que suas organizações estão se adaptando à regulamentação, embora a adoção de práticas de engenharia de privacidade estruturadas ainda seja limitada. Métodos informais e a falta de ferramentas durante a elicitação de requisitos de privacidade são predominantes, refletindo a necessidade de maior conscientização, treinamento focado e recursos práticos para conectar o conhecimento teórico à implementação no mundo real.

Uma pesquisa futura deve focar em conectar as lacunas identificadas, investigando a escalabilidade, adaptabilidade e efetividade dessas técnicas, métodos, processos, *frameworks*

e ferramentas em diversos ambientes de software reais. Esses esforços devem aumentar a solidez das práticas de preservação de privacidade na fase de engenharia de requisitos e contribuir para o desenvolvimento de sistemas de software voltados à privacidade, que atendam tanto às normas regulatórias quanto às expectativas dos usuários.

Referências

[1] 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

[2] 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

[3] 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, 6, 39

[4] 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, 39

[5] Parliament, The European e The Council: *General Data Protection Regulation (GDPR).* Intersoft Consulting, 2018. https://gdpr-info.eu. 1, 2, 5, 22, 36

[6] Republic, Brazil Presidency of the: *Law no. 13,709 of august 14, 2018. brazilian data protection law (lgpd).* Official Daily of the Federative Republic of Brazil, 2018. https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/lgpd-en-lei-no-13-709-capa.pdf/. 1, 2, 4, 5, 22

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

[8] Pfleeger, Charles P: *Security in computing.* Prentice-Hall, Inc., 1988. 2

[9] Breaux, Travis D.: *Privacy requirements in an age of increased sharing.* IEEE Softw., 31(5):24–27, 2014. https://doi.org/10.1109/MS.2014.118. 2

[10] 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

[11] 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

[12] Radics, Peter J. e Denis Gracanin: *Privacy in domestic environments.* Em *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

[13] 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, 5

[14] 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 *ICEIS (1)*, páginas 19–30, 2021. 2

[15] Alkubaisy, Duaa, Karl Cox e Haralambos Mouratidis: *Towards detecting and mitigating conflicts for privacy and security requirements.* Em *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

[16] Thomas, Keerthi, Arosha K. Bandara, Blaine A. Price e Bashar Nuseibeh: *Distilling privacy requirements for mobile applications.* Em *36th International Conference on Software Engineering, ICSE '14, Hyderabad, India - May 31 - June 07, 2014*, páginas 871–882. ACM, 2014. https://doi.org/10.1145/2568225.2568240. 2

[17] Benjamins, Richard: *Towards organizational guidelines for the responsible use of AI.* Em *ECAI 2020 - 24th European Conference on Artificial Intelligence, 29 August-8 September 2020, Santiago de Compostela, Spain, August 29 - September 8, 2020 - Including 10th Conference on Prestigious Applications of Artificial Intelligence (PAIS 2020)*, volume 325 de *Frontiers in Artificial Intelligence and Applications*, páginas 2879–2880. IOS Press, 2020. https://doi.org/10.3233/FAIA200433. 2

[18] 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. 3, 6

[19] 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. 4, 19, 27

[20] 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. 4, 16, 25, 27, 32

[21] Silva, Deógenes P, 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 *Proceedings of the 17th Brazilian Symposium on Human Factors in Computing Systems*, páginas 1–10, 2018. 4, 17, 25, 32, 33

[22] 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`. 4, 17, 27, 29, 30, 31, 32

[23] Alves, Carina e Moisés Neves: *Especificação de requisitos de privacidade em conformidade com a lgpd: Resultados de um estudo de caso.* Em *WER*, 2021. 5, 20, 25

[24] 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`. 5

[25] 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`. 5

[26] Ferrao, Sâmmara Éllen Renner e Edna Dias Canedo: *Uma taxonomia para requisitos de privacidade e sua aplicação no open banking brasil.* Em *WER*, 2022. 6, 20, 25

[27] Santos, Arthur, Mariana Peixoto e Carla Silva: *Um modelo de conceitos relacionados à privacidade de dados pessoais.* 6, 20

[28] 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`. 6

[29] 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. 7

[30] Meis, Rene e Maritta Heisel: *Computer-aided identification and validation of privacy requirements*. Inf., 7(2):28, 2016. https://doi.org/10.3390/info7020028. 7

[31] 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. 7

[32] Keele, Staffs *et al.*: *Guidelines for performing systematic literature reviews in software engineering*, 2007. 8, 11, 42

[33] 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. 9

[34] 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. 9, 42

[35] 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. 15, 32, 35

[36] Beckers, Kristian e Maritta Heisel: *A foundation for requirements analysis of privacy preserving software*. Em *Multidisciplinary Research and Practice for Information Systems*, páginas 93–107, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg, ISBN 978-3-642-32498-7. 15, 32, 33

[37] 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. 15, 27, 28, 30, 31, 32, 35

[38] 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. 15, 27, 30, 31, 32, 33

[39] 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. 15, 27, 32, 35

[40] 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 *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`. 15, 27, 32, 35

[41] Hung, Patrick CK, Marcelo Fantinato e Laura Rafferty: *A study of privacy requirements for smart toys*. Pacific Asia Conference on Information Systems (PACIS), 2016. 16, 32

[42] Sangaroonsilp, Pattaraporn, Hoa Khanh Dam, Morakot Choetkiertikul, Chaiyong Ragkhitwetsagul e Aditya Ghose: *A taxonomy for mining and classifying privacy requirements in issue reports*. Information and Software Technology, 157:107162, 2023. 16, 25, 30, 31, 32, 33

[43] Bijwe, Ashwini e Nancy R Mead: *Adapting the square process for privacy requirements engineering*. Software Engineering Institute: Pittsburgh, PA, USA, 2010. 16, 27, 32

[44] Kalloniatis, Christos, Evangelia Kavakli e Stefanos Gritzalis: *Addressing privacy requirements in system design: the pris method*. Requirements Engineering, 13:241–255, 2008. 16, 25, 27, 28, 32

[45] 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. 16, 34

[46] 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. 16, 27, 30, 31, 32, 35

[47] 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. 16, 30, 31, 32, 34

[48] 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. 16, 25, 27, 32

[49] 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. 16, 26, 27, 30, 31, 32, 36

[50] Olukoya, Oluwafemi: *Assessing frameworks for eliciting privacy & security requirements from laws and regulations.* Computers & Security, 117:102697, 2022. 16, 32

[51] 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. 16, 25, 26, 32

[52] Beckers, Kristian: *Comparing privacy requirements engineering approaches.* Em *2012 Seventh International Conference on Availability, Reliability and Security*, páginas 574–581. IEEE, 2012. 16, 27, 32

[53] 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. 16, 25, 27, 30, 31, 32, 34

[54] 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. 16, 27, 30, 31, 32

[55] 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. 16, 27, 30, 31, 32, 34

[56] 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. 16, 32

[57] Gharib, Mohamad, Paolo Giorgini e John Mylopoulos: *Copri v. 2—a core ontology for privacy requirements.* Data & Knowledge Engineering, 133:101888, 2021. 16, 27, 32, 35

[58] 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. 16, 30, 31, 32

[59] 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. 16, 26, 27, 30, 31, 32

[60] 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. 17, 30, 31

[61] 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. 17, 27, 32

[62] 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. 17, 34

[63] 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. 17, 32

[64] 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. 17, 30, 31, 32

[65] Sindre, Guttorm e Andreas L Opdahl: *Eliciting security requirements with misuse cases*. Requirements engineering, 10:34–44, 2005. 17, 32

[66] Krishnan, Padmanabhan e Kostyantyn Vorobyov: *Enforcement of privacy requirements*. Computers & Security, 52:164–177, 2015. 17, 30, 31, 32

[67] Spiekermann, Sarah e Lorrie Faith Cranor: *Engineering privacy*. IEEE Transactions on software engineering, 35(1):67–82, 2008. 17, 25, 32, 34

[68] 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. 17, 27, 30, 31, 32, 34

[69] 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. 17, 25, 27, 30, 31, 32

[70] Kalloniatis, Christos, Haralambos Mouratidis e Shareeful Islam: *Evaluating cloud deployment scenarios based on security and privacy requirements*. Requirements Engineering, 18:299–319, 2013. 17, 27, 32, 33

[71] 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. 17, 27, 28, 30, 31

[72] Zimmermann, Christian: *Framework and requirements for reconciling digital services and privacy*. European Conference on Information Systems (ECIS), 2016. 17, 32

[73] Schlehahn, Eva e Rigo Wenning: *GDPR Transparency Requirements and Data Privacy Vocabularies*, páginas 95–113. Springer International Publishing, Cham, 2019, ISBN 978-3-030-16744-8. https://doi.org/10.1007/978-3-030-16744-8_7. 17

[74] 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. 17, 27, 32

[75] 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. 17, 27, 32

[76] 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. 17, 27, 30, 31, 32

[77] Herwanto, Guntur Budi, Gerald Quirchmayr e A Min Tjoa: *Leveraging nlp techniques for privacy requirements engineering in user stories*. IEEE Access, 2024. 17, 25, 30, 31, 32, 34

[78] 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. 18, 27, 32

[79] 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. 18, 25, 27, 30, 31, 32, 33

[80] 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. 18, 30, 31, 32

[81] 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. 18, 25, 30, 31, 32

[82] 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. 18, 27, 30, 31, 32

[83] 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. 18, 32, 33

[84] 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. 18, 32

[85] Kalloniatis, Christos, Evangelia Kavakli e Efstathios Kontellis: *Pris tool: A case tool for privacy-oriented requirements engineering.* Em *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`. 18, 27, 32

[86] Hörbe, Rainer e Walter Hötzendorfer: *Privacy by design in federated identity management.* Em *2015 IEEE Security and Privacy Workshops*, páginas 167–174. IEEE, 2015. 18, 25, 27, 32

[87] 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. 18, 25, 31, 32

[88] 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`. 18, 32, 36

[89] 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. 18, 32

[90] 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. 18, 32, 34

[91] 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. 18, 32

[92] 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. 18, 30, 31, 32

[93] 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. 18, 25, 36

[94] 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. 18

[95] 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. 18, 27, 32

[96] 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. 18, 25, 27, 30, 31, 32

[97] 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. 18, 25, 32

[98] 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. 19, 25, 32

[99] 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. 19, 27, 28, 32

[100] 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. 19, 25, 32, 33

[101] 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. 19, 25, 26

[102] 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. 19, 27, 30, 31, 32

[103] 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. 19, 32

[104] 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. 19, 27, 28, 30, 31, 32

[105] Jensen, Carlos, Joe Tullio, Colin Potts e Elizabeth D Mynatt: *Strap: a structured analysis framework for privacy.* Georgia Institute of Technology, 1, 2005. 19, 27, 29, 30, 31, 32

[106] 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. 19, 25, 27, 32

[107] 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. 19, 30, 31, 32, 34

[108] 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. 19, 27, 32, 36

[109] Peixoto, Mariana Maia, Carla Silva, Helton Maia e Joao Araújo: *Towards a catalog of privacy related concepts.* Em *REFSQ Workshops*, 2020. 19, 25, 27, 30, 31, 32

[110] 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. 19, 27, 28, 32

[111] 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. 19, 25, 32

[112] 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. 19, 25, 30, 31, 32, 34

[113] 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. 19, 25, 32, 35

[114] 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. 19, 27, 29, 30, 31

[115] Ferraris, Davide e Carmen Fernandez-Gago: *Trustapis: a trust requirements elicitation method for iot.* International Journal of Information Security, 19(1):111–127, 2020. 19, 25, 26, 27, 32

[116] 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. 19, 32

[117] 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. 20, 27, 32

[118] 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. 20, 25

[119] 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. 20, 30, 31

[120] 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.* 20

[121] 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. 20, 25, 30, 31

[122] 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. 20, 25, 30, 31

[123] Santana, Egberto, Jéssyka Vilela e Mariana Maia Peixoto: *Diretrizes para apresentação de políticas de privacidade voltadas à experiência do usuário.* Em *WER*, 2022. 20

[124] 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. 20

[125] 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. 20

[126] 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. 20, 25, 30, 31

[127] 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. 20

[128] 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. 20, 25, 30, 31

[129] 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.* 20

[130] 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. 21, 25

[131] 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. 21

[132] 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. 21, 25, 26, 32

[133] Bondel, Gloria, Gonzalo Munilla Garrido, Kevin Baumer e Florian Matthes: *Towards a privacy-enhancing tool based on de-identification methods.* Pacific Asia Conference on Information Systems (PACIS), 2020. 21, 32

[134] 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. 21

[135] 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 *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. 21, 25

[136] 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. 21, 32

[137] Diamantopoulou, V, A Androutsopoulou, S Gritzalis e Y Charalabidis: *Preserving digital privacy in e-participation environments: Towards gdpr compliance. information, 11 (2), 117*, 2020. 21, 25, 27, 32

[138] 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. 21, 32

[139] Belhajjame, Khalid, Noura Faci, Zakaria Maamar, Vanilson Burégio, Edvan Soares e Mahmoud Barhamgi: *On privacy-aware escience workflows.* Computing, 102:1171–1185, 2020. 21, 32

[140] 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. 21, 25

[141] 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. 21, 32

[142] 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. 21, 32

[143] 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. 21, 27, 32

[144] 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. 21, 25, 27, 32

[145] 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. 21, 32

[146] 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. 21, 27, 32

[147] 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. 21, 25, 32

[148] 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. 22, 32

[149] 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. 22, 25, 30, 31, 32

[150] 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. 22, 32

[151] 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 *Requirements Engineering: Foundation for Software Quality*, páginas 92–108, Cham, 2024. Springer Nature Switzerland, ISBN 978-3-031-57327-9. 22, 32

[152] Herwanto, Guntur Budi, Gerald Quirchmayr e A. Min Tjoa: *Learning to rank privacy design patterns: A semantic approach to meeting privacy requirements*. Em *Requirements Engineering: Foundation for Software Quality*, páginas 57–73, Cham, 2024. Springer Nature Switzerland, ISBN 978-3-031-57327-9. 22, 32

[153] 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. 22

[154] 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. 27

[155] 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. 28

[156] 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. 29

[157] 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`. 40