

A Engenharia de Requisitos e a Lei Geral de Proteção de Dados (LGPD): Uma Revisão Sistemática da Literatura

Eduarda Elger
Universidade Estadual do Oeste do Paraná - Unioeste
Cascavel, Brasil
eduarda.elger@unioeste.br

Victor Araya Santander
Universidade Estadual do Oeste do Paraná - Unioeste
Cascavel, Brasil
victor.santander@unioeste.br

Abstract—In September 2020, the General Data Protection Law (LGPD) came into force in Brazil, regulating the processing of data in physical and digital media, both in public and private institutions, with the primary objective of ensuring privacy and individual rights. Given this scenario, requirements engineering turns its attention to the influence of the LGPD in the early stages of software development, especially in the scope of non-functional requirements (NFR). This work proposes an approach based on the planning and execution stages of a systematic literature review (SLR) to analyze methods, techniques, and studies used in requirements engineering, with a focus on the non-functional requirement of privacy, aiming at compliance with the LGPD.

Keywords—General Data Protection Law (LGPD); Non-Functional Requirements (NFR); Requirements Engineering; Systematic Review (RSL).

Resumo—Em setembro de 2020, a Lei Geral de Proteção de Dados (LGPD) entrou em vigor no Brasil, regulamentando o tratamento de dados em meios físicos e digitais, tanto em instituições públicas quanto privadas, com o objetivo primordial de assegurar a privacidade e os direitos individuais. Diante desse cenário, a engenharia de requisitos direciona sua atenção para a influência da LGPD nas fases iniciais do desenvolvimento de software, especialmente no âmbito dos requisitos não-funcionais (NFR). Este trabalho propõe uma abordagem baseada nas etapas de planejamento e execução de uma revisão sistemática da literatura (RSL) para analisar métodos, técnicas e estudos utilizados na engenharia de requisitos, com foco no requisito não-funcional de privacidade, visando a conformidade com a LGPD.

Palavras-chave— Lei Geral de Proteção de Dados (LGPD); Requisitos Não-Funcionais (NFR); Engenharia de Requisitos; Revisão Sistemática (RSL).

I. INTRODUÇÃO

A era digital trouxe consigo uma transformação profunda na maneira como lidamos com informações pessoais. À medida que a tecnologia avança, a quantidade de dados sensíveis gerados e compartilhados cresce exponencialmente, acompanhada de preocupações crescentes sobre a segurança e privacidade dessas informações. Em resposta a essa crescente preocupação global, a legislação de proteção de dados desempenha um papel fundamental na regulamentação do tratamento dessas informações sensíveis.

A Lei Geral de Proteção de Dados Pessoais (LGPD) estabelece diretrizes importantes e obrigatórias para a coleta, processamento e armazenamento de dados pessoais. Ela foi inspirada na GDPR (General Data Protection Regulation) [1],

que entrou em vigência em 2018 na União Europeia, trazendo grandes impactos para empresas e consumidores [2]. No cenário brasileiro, a LGPD, em vigor desde setembro de 2020, representa um marco significativo na proteção da privacidade e segurança dos dados pessoais [3]. Esta legislação estabelece diretrizes rigorosas para o tratamento de informações pessoais por organizações públicas e privadas, impactando diretamente a forma como o desenvolvimento de software lida com a engenharia de requisitos.

Por outro lado, a engenharia de requisitos de software [4] demonstra preocupação em relação ao impacto que sofrerá nos estágios iniciais do desenvolvimento de software. Esse impacto atinge diretamente a coleta, tratamento e armazenamento de dados, especialmente no que diz respeito aos requisitos não-funcionais. Os requisitos não-funcionais, originados das necessidades dos usuários e de fatores externos como regulamentos de segurança ou legislações de privacidade [5], agora precisam incorporar considerações explícitas sobre privacidade e conformidade legal devido à LGPD.

Destaca-se o trabalho significativo sobre requisitos não-funcionais, como o NFR Framework, que separa o conceito de funcionalidade de outros atributos de qualidade e preocupações relacionadas à produtividade, tempo e custo, por meio de um nível mais alto de abstração [6]. Este framework oferece uma abordagem estruturada para lidar com requisitos não-funcionais, fornecendo uma base sólida para incorporar considerações de privacidade e conformidade legal na engenharia de requisitos em resposta aos desafios impostos pela LGPD. Essa abordagem mais abrangente e estruturada é essencial para garantir a conformidade e a eficácia no desenvolvimento de software em conformidade com os requisitos legais e as preocupações éticas emergentes.

A LGPD estabelece uma série de princípios que devem ser observados por aqueles que lidam com dados pessoais, tais como transparência, finalidade, adequação, necessidade, livre acesso, qualidade dos dados, segurança, prevenção, não discriminação e responsabilização. Estes princípios são fundamentais para garantir a privacidade e a proteção dos dados pessoais dos titulares, e devem ser aplicados desde a coleta até o descarte desses dados [7].

A transparência na documentação dos requisitos é vital não apenas para o processo de desenvolvimento, mas também

para atender às demandas legais. É fundamental que as empresas e organizações se adaptem à LGPD e implementem medidas de segurança e privacidade para garantir a proteção dos dados pessoais de seus clientes e usuários, além de proteger a própria organização contra possíveis sanções [8]. Profissionais de engenharia de requisitos desempenham um papel essencial, garantindo a compreensão e implementação adequada dos requisitos relacionados à LGPD. Ignorar essas considerações pode resultar em sistemas que não apenas violam a legislação, mas também enfrentam penalidades legais e prejudicam a reputação da organização. Portanto, é imperativo que a engenharia de requisitos evolua para incorporar considerações legais e éticas, assegurando que o software não apenas atenda aos requisitos funcionais, mas também esteja em conformidade com as normas regulatórias, como a LGPD. Diante desse contexto, a engenharia de requisitos de software desempenha um papel crucial na garantia da conformidade com a LGPD. Ela precisa incorporar requisitos relacionados à proteção de dados desde o início do ciclo de desenvolvimento, assegurando que sistemas e produtos sejam projetados e operados de acordo com os princípios de privacidade e segurança estabelecidos por essa legislação. Portanto, a LGPD não apenas impulsiona a preocupação com a proteção de dados, mas também molda profundamente a abordagem e práticas da engenharia de requisitos, tornando-a essencial para a conformidade e para a preservação da privacidade dos indivíduos.

Além desta seção, na seção II apresenta-se o referencial teórico necessário para o entendimento do trabalho, na seção III a metodologia adotada que consiste nos passos para a realização da RSL e na seção IV a análise e síntese dos resultados. Finalmente, na seção V são apresentadas as considerações finais do trabalho.

II. REFERENCIAL BIBLIOGRÁFICO

A. Revisão Sistemática da Literatura

A Revisão Sistemática da Literatura (RSL), também conhecida como Revisão Sistemática (RS), tem como objetivo realizar a sumarização dos estudos disponíveis sobre um determinado assunto até o momento da revisão. Através dela, são executadas etapas como identificação, seleção, avaliação, interpretação e sumarização desses estudos. A RSL é considerada um estudo secundário, o que significa que os estudos utilizados em sua elaboração são denominados estudos primários. Esses estudos primários são os trabalhos individuais que servem como base e são analisados durante o processo da RSL [9].

Com suas origens na área da Medicina [10], a Revisão Sistemática da Literatura (RSL) foi incorporada ao cenário da Engenharia de Software em 2004, sob a orientação de [11]. Desde então, a RSL tem experimentado um reconhecimento crescente tanto na comunidade de Engenharia de Software quanto na ampla esfera da Ciência da Computação. O processo de condução de uma RSL é delineado por uma série de passos definidos, conforme ilustrado na Figura 1.

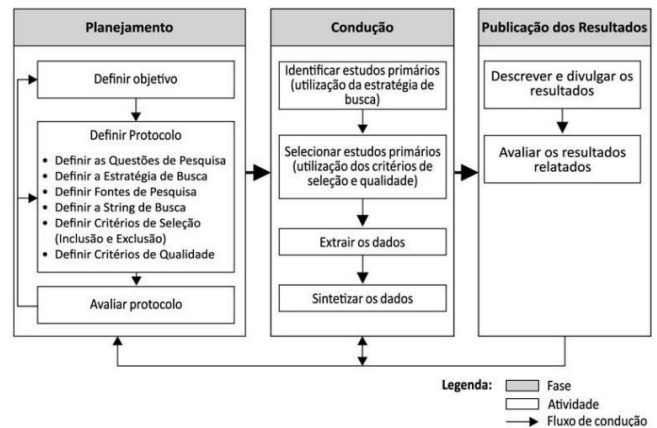


Fig. 1. Fases e atividades do processo de uma RSL [12].

B. Lei Geral de Proteção de Dados

Lei Geral de Proteção de Dados (LGPD), oficialmente conhecida como Lei nº 13.709/2018 [3], representa uma legislação abrangente no Brasil que regulamenta o tratamento de dados pessoais no país. Promulgada em 14 de agosto de 2018, LGPD foi inspirada pelo Regulamento Geral de Proteção de Dados (GDPR) da União Europeia [1], cujos debates em torno dos assuntos abordados no Regulamento são oriundos dos anos 90, com a edição da Diretiva 95/46/CE da Comunidade Europeia, principal documento acerca da proteção da privacidade do ser humano no âmbito internacional. Por conta disso, o GDPR é um diploma legal mais completo e detalhista do que a lei brasileira [13]. Seu propósito fundamental é estabelecer princípios, direitos e obrigações relacionados ao uso de informações pessoais, visando a proteção da privacidade e liberdade individuais. Até o momento, 128 países em todo o mundo já implementaram legislação para assegurar a proteção de dados e a privacidade [14].

A LGPD entrou em vigor em setembro de 2020, após um período de adaptação. Seus aspectos cruciais incluem a necessidade de obtenção de consentimento explícito para o tratamento de dados, a garantia dos direitos dos titulares das informações, a notificação obrigatória em incidentes de segurança, além da criação da Autoridade Nacional de Proteção de Dados (ANPD), responsável por fiscalizar e aplicar as normas da legislação [15]. A lei abrange o tratamento de dados pessoais em ambientes físicos e digitais, visando salvaguardar direitos fundamentais como liberdade, privacidade e desenvolvimento da personalidade [14]. Além disso, a Lei Geral de Proteção de Dados (LGPD) é subdividida em 10 capítulos, que totalizam 65 artigos. Esses capítulos abordam temas fundamentais, como os direitos dos titulares, obrigações dos controladores e as sanções aplicáveis. Embora a LGPD tenha sido influenciada pela GDPR, elas apresentam diferenças significativas. Enquanto a LGPD é composta por 10 capítulos e 65 artigos, conforme ilustrado na Tabela I, a GDPR possui 11 capítulos e 99 artigos. Essa disparidade indica que a GDPR é mais abrangente e detalhada em comparação com a legislação brasileira, evidenciando uma maior complexidade e amplitude de abordagem na proteção de dados.

TABELA I
ARTIGOS DA LGPD

Capítulo	Artigo	Disposição
I	1º	Esta Lei regula o tratamento de dados pessoais para garantir a proteção dos direitos de liberdade, privacidade e o desenvolvimento da personalidade.
I	2º	Estabelece os fundamentos da disciplina de proteção de dados pessoais.
I	3º	Define a aplicação ao tratamento de dados realizado por pessoas ou empresas no Brasil, ou referente a dados de indivíduos no país, desde que coletados no Brasil.
I	4º	Estabelece as exceções da aplicação da Lei, como tratamento para fins exclusivamente particulares, jornalísticos, acadêmicos, segurança pública, defesa nacional e dados provenientes de fora do país com adequado grau de proteção.
I	5º	Define termos importantes para a compreensão da Lei, como dado pessoal, dado pessoal sensível, banco de dados, titular, controlador, operador, encarregado, tratamento, consentimento, entre outros.
I	6º	Estabelece os princípios que devem guiar as atividades de tratamento de dados pessoais, como finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas.
II	7º	Tratamento de dados pessoais somente pode ocorrer com consentimento, obrigação legal, necessidades de políticas públicas, estudos de pesquisa, contratos, direitos judiciais ou para proteção.
II	8º	Consentimento deve ser obtido por escrito ou de forma manifesta; responsabilidade do controlador provar a obtenção adequada do consentimento.
II	9º	Direito do titular ao acesso facilitado às informações sobre o tratamento de seus dados.
II	10º	O legítimo interesse do controlador só pode fundamentar tratamento de dados para finalidades legítimas.
II	11º	Tratamento de dados sensíveis requer consentimento específico ou em circunstâncias específicas.
II	12º	Dados anonimizados não são considerados dados pessoais, salvo reversão do processo de anonimização.
II	13º	Acesso a dados pessoais em estudos de saúde pública sob condições específicas e garantias de segurança.
II	14º	Tratamento de dados de crianças e adolescentes deve ser no melhor interesse deles, com consentimento dos pais.
II	15º	Término do tratamento de dados ocorre quando finalidade é alcançada, dados não são

		mais necessários ou por determinação da autoridade nacional.
II	16º	Eliminação dos dados após o fim do tratamento, salvo exceções permitidas.
III	17º	Titulares têm direitos fundamentais de liberdade, intimidade e privacidade sobre seus dados.
III	18º	Direitos do titular incluem acesso, correção, anonimização, portabilidade, eliminação e revogação de consentimento.
III	19º	Direito do titular à confirmação de existência e acesso a dados, com prazos e formatos específicos.
III	20º	Direito do titular à revisão de decisões baseadas em tratamento automatizado de dados pessoais.
III	21º	Dados pessoais do titular não podem ser usados contra ele no exercício regular de seus direitos.
III	22º	A defesa dos direitos dos titulares pode ser exercida individual ou coletivamente em juízo.
IV	23º	O tratamento de dados pelo poder público deve visar ao interesse público, com divulgação clara e designação de encarregado.
IV	24º	Empresas públicas e sociedades de economia mista são tratadas como entidades privadas, exceto em políticas públicas.
IV	25º	Dados devem ser mantidos em formato interoperável para uso compartilhado e acesso público.
IV	26º	Uso compartilhado de dados pelo Poder Público deve ter finalidades específicas e respeitar princípios de proteção.
IV	27º	Comunicação de dados públicos para privados requer consentimento do titular, salvo exceções e dispensas previstas.
IV	29º	A Autoridade Nacional pode solicitar informações detalhadas sobre tratamento de dados pelo Poder Público.
IV	30º	A Autoridade Nacional pode estabelecer normas complementares para comunicação e uso compartilhado de dados pelo Poder Público.
IV	31º	A Autoridade Nacional pode intervir em caso de violação da Lei no tratamento de dados por órgãos públicos.
IV	32º	A Autoridade Nacional pode solicitar relatórios de impacto e promover boas práticas no tratamento de dados pelo Poder Público.
V	33º	A transferência internacional de dados pessoais é permitida em certos casos, incluindo consentimento do titular.
V	34º	O nível de proteção de dados do país estrangeiro será avaliado pela autoridade nacional antes da transferência.
V	35º	A autoridade nacional é responsável pela definição e verificação de cláusulas contratuais e outras garantias.
V	36º	Alterações nas garantias de proteção de dados

		deverem ser comunicadas à autoridade nacional.
VI	37º	Controlador e operador devem manter registro das operações de tratamento de dados pessoais.
VI	38º	A autoridade nacional pode solicitar ao controlador um relatório de impacto à proteção de dados pessoais.
VI	39º	O operador deve realizar o tratamento de acordo com as instruções do controlador.
VI	40º	A autoridade nacional pode estabelecer padrões para interoperabilidade, portabilidade, livre acesso aos dados e segurança.
VI	41º	O controlador deve indicar um encarregado pelo tratamento de dados pessoais, cujas informações devem ser divulgadas publicamente.
VI	42º	O controlador ou operador é obrigado a reparar danos causados pelo tratamento de dados, solidariamente em certas circunstâncias.
VI	43º	Os agentes de tratamento não são responsabilizados em casos específicos, como quando não realizam o tratamento atribuído.
VI	44º	O tratamento de dados pessoais é irregular quando não segue a legislação ou não fornece a segurança esperada pelo titular.
VI	45º	As violações dos direitos do titular nas relações de consumo seguem as regras de responsabilidade da legislação pertinente.
VII	46º	Agentes de tratamento devem adotar medidas de segurança para proteger os dados pessoais.
VII	47º	A segurança da informação prevista na Lei deve ser garantida mesmo após o término do tratamento.
VII	48º	O controlador deve comunicar à autoridade nacional e ao titular incidentes de segurança relevantes.
VII	49º	Os sistemas de tratamento de dados devem atender a requisitos de segurança e padrões de boas práticas.
VII	50º	Controladores e operadores podem formular regras de boas práticas e governança para o tratamento de dados pessoais.
VII	51º	A autoridade nacional deve estimular a adoção de padrões técnicos que facilitem o controle dos dados pelos titulares.
VIII	52º	Os agentes de tratamento estão sujeitos a sanções administrativas por infrações à Lei, incluindo advertência, multa, publicização da infração, entre outras.
VIII	53º	A autoridade nacional definirá metodologias para calcular o valor-base das multas por infrações à Lei, sujeitas a consulta pública.
VIII	54º	O valor da multa diária por infrações à Lei deve ser proporcional à gravidade da falta e ao dano causado, fundamentado pela autoridade nacional.
IX	55º-A -B	Artigo vetado.

IX	55º-C	Composição da ANPD, incluindo Conselho Diretor, Corregedoria, Ouvidoria, Procuradoria e unidades administrativas especializadas.
IX	55º-D	Composição do Conselho Diretor da ANPD, incluindo 5 diretores, sendo um Diretor-Presidente, com mandato de 4 anos.
IX	55º-E	Condições para perda de cargo dos membros do Conselho Diretor da ANPD.
IX	55º-F	Aplicação de normas de conduta aos membros do Conselho Diretor após o exercício do cargo.
IX	55-G	Ato do Presidente da República disporá sobre a estrutura regimental da ANPD.
IX	55-H	Remanejamento de cargos em comissão e funções de confiança para a ANPD.
IX	55-I	Indicação e nomeação dos ocupantes de cargos em comissão e funções de confiança da ANPD.
IX	55-J	Competências da ANPD, incluindo proteção de dados, fiscalização, elaboração de diretrizes e promoção do conhecimento sobre proteção de dados.
IX	55-K	A ANPD é responsável pela aplicação das sanções previstas na Lei, prevalecendo suas competências sobre outras entidades públicas.
IX	55-L	Fontes de receita da ANPD, incluindo dotações orçamentárias, doações, venda de bens, entre outros.
IX	55-M	Determinação sobre o patrimônio da ANPD.
IX	56º; 57º	Artigo vetado.
IX	58-A	Composição do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, incluindo representantes de diversos órgãos e entidades.
IX	58-B	Competências do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, incluindo proposição de diretrizes e disseminação de conhecimento.
IX	59º	Artigo vetado.
X	60º	Alterações no Marco Civil da Internet, incluindo a exclusão definitiva de dados pessoais fornecidos a uma aplicação de internet ao término da relação entre as partes.
X	61º	Notificação e intimação de empresas estrangeiras de todos os atos processuais previstos na Lei, na pessoa de seu representante no Brasil.
X	62º	Edição de regulamentos específicos pela autoridade nacional e pelo Inep para o acesso a dados tratados pela União, relacionados à educação.
X	63º	Estabelecimento de normas pela autoridade nacional para a adequação progressiva de bancos de dados constituídos até a entrada em vigor da Lei.
X	64º	Reconhecimento de que os direitos e princípios expressos na Lei não excluem outros previstos na legislação nacional ou em

		tratados internacionais.
X	65º	Entrada em vigor da Lei, com especificações temporais para diferentes artigos.

A conformidade com a LGPD é essencial para empresas e organizações que lidam com dados pessoais, e o não cumprimento das disposições legais pode resultar em penalidades significativas, sendo elas, multa de até 2% do faturamento, com limite de até R\$ 50 milhões; o bloqueio ou a eliminação dos dados pessoais relacionados à irregularidade, a suspensão parcial do funcionamento do banco de dados ou a proibição parcial ou total da atividade de tratamento [17]. Em julho de 2023, a Autoridade Nacional de Proteção de Dados (ANPD) aplicou a primeira multa por descumprimento da Lei Geral de Proteção de Dados (LGPD). A penalidade foi dirigida à empresa do ramo de telefonia, com um valor fixado em R\$14.400,00, limitado a 2% do seu faturamento bruto [18].

C. Engenharia de Requisitos

A Engenharia de Requisitos é considerada uma das etapas do processo de desenvolvimento de software em que o analista procura compreender quais são as reais necessidades dos clientes no que tange à resolução ou dissolução do problema posto em foco. Tal área pode ser descrita como um conjunto de atividades para descobrir, analisar, documentar e verificar os requisitos e artefatos gerados, ressaltando que as atividades podem variar de uma organização para outra, ou até mesmo dentro de uma mesma organização, em razão das particularidades de cada projeto [4].

Os requisitos delineiam as ações que o sistema deve realizar e as condições sob as quais deve operar. Os requisitos associados à funcionalidade do sistema, ou seja, o que o sistema deve fazer, são denominados Requisitos Funcionais. Em contrapartida, os requisitos ligados às condições sob as quais o sistema deve operar são designados como Requisitos Não-Funcionais [19].

Os requisitos não funcionais, conforme o próprio nome sugere, não se relacionam diretamente com os serviços específicos oferecidos pelo sistema aos seus usuários. Em vez disso, eles podem estar associados a propriedades emergentes do sistema, tais como confiabilidade, tempo de resposta e eficiência de ocupação de recursos. A origem dos requisitos não funcionais pode estar nas necessidades dos usuários, restrições de orçamento, políticas organizacionais, exigências de interoperabilidade com outros sistemas de software ou hardware, bem como fatores externos como regulamentos de segurança ou legislações de privacidade.

O requisito de privacidade, delineado por [5], representa as diretrizes fundamentais para preservar a integridade da privacidade dos dados ao longo do ciclo de vida do desenvolvimento de software. No contexto da engenharia de requisitos [20], esse requisito desempenha um papel crucial ao estabelecer normativas para o tratamento ético, seguro e transparente das informações pessoais dos usuários, desde a fase inicial de coleta de dados até a implementação de

medidas de segurança. O objetivo é garantir a conformidade legal e atender às expectativas dos usuários em relação à salvaguarda de seus dados sensíveis. A implementação eficaz desse requisito não apenas assegura a conformidade legal, mas também contribui para a construção de sistemas digitais confiáveis, éticos e alinhados com as necessidades e preocupações dos usuários.

A importância da identificação e modelagem correta do requisito de privacidade durante a fase de desenvolvimento de software garante um software com um grau significativo de proteção da privacidade dos dados dos usuários [21]. A teoria da privacidade na engenharia de requisitos [22], destaca a relevância dos requisitos não funcionais, nos quais a privacidade emerge como uma dimensão essencial. Esse requisito não funcional é formulado para assegurar que o sistema respeite e proteja adequadamente as informações pessoais dos usuários, indo além das funcionalidades específicas para abordar propriedades emergentes, como confiabilidade e desempenho. No âmbito da privacidade, esse requisito abrange desde a coleta inicial de dados até a aplicação de medidas de segurança robustas, incluindo transparência no tratamento de dados, segurança da informação e conformidade com legislações específicas, como a Lei Geral de Proteção de Dados (LGPD) e o Regulamento Geral de Proteção de Dados (GDPR).

III. METODOLOGIA

A. Planejamento da Revisão Sistemática

A fase inicial de uma Revisão Sistemática da Literatura (RSL) destaca a importância do planejamento e do desenvolvimento de um protocolo. A relevância dessa fase reside no fato de que, por meio das questões de pesquisa, todo o protocolo é orientado, moldando a abordagem da revisão e direcionando a busca por informações relevantes [24]. Este protocolo, dividido em cinco seções, orienta a execução da revisão e inclui a apresentação da ferramenta Parsifal [23], que apoia tanto o planejamento quanto a execução do protocolo. A definição de questões de pesquisa, utilizando o método PICOC, é enfatizada como uma etapa crucial, guiando a busca por informações relevantes. Os objetivos gerais e específicos da RSL são definidos, incluindo a exploração da engenharia de requisitos em conformidade com a Lei Geral de Proteção de Dados (LGPD). Os objetivos específicos incluem planejar e executar o protocolo da RSL com o apoio da ferramenta Parsifal, separar artigos relevantes sobre engenharia de requisitos e LGPD, e identificar temas significativos no estudo. O método PICOC foi definido de acordo com o tema da presente RSL, conforme segue.

Population: Trabalhos na engenharia de requisitos.

Intervention: Métodos, técnicas, estudos, relatos de experiências.

Comparison: não se aplica.

Outcome: Analisar métodos, técnicas e estudos utilizados na engenharia de requisitos para ficar em conformidade com a LGPD e GDPR.

Context: Adequação das atividades do processo de engenharia de requisitos à legislação de proteção de dados.

A identificação de estudos envolve a criação de uma *string* de busca e a seleção de bases de dados, resultando na identificação de 996 trabalhos relevantes. As questões de pesquisa formuladas para a RSL incluem: o que a engenharia de requisitos tem proposto para se adequar às exigências da LGPD; o entendimento de privacidade na LGPD e sua relação com a engenharia de requisitos; e a adaptação de soluções da engenharia de requisitos para atender a exigências de leis internacionais como a GDPR. Os critérios de inclusão e exclusão são estabelecidos, considerando o período de 2016 a 2023, e a qualidade dos estudos é avaliada com base em questões específicas. Essa abordagem robusta, juntamente com a eficácia da ferramenta Parsifal, contribui para uma organização eficiente do processo de revisão, preparando o terreno para a fase de execução da RSL.

B. Execução da Revisão Sistemática

A etapa inicial da importação de estudos na Revisão Sistemática da Literatura (RSL) começa com a aplicação de uma *string* de busca definida no planejamento. Essa *string* é utilizada em várias bases de dados, considerando apenas publicações de 2016 a 2023. Filtros adicionais excluem estudos duplicados e garantem que apenas aqueles com termos-chave relevantes sejam incluídos, aprimorando a qualidade da análise. A importação é realizada por meio de arquivos BibTeX gerados pelas bases de dados, contendo informações essenciais para a revisão.

Dentre as bases de dados consultadas, a ACM Digital Library inicialmente apresentou 91 estudos, resultando em 90 após remoção de duplicatas. A base EI Compendex identificou 88 estudos, com 35 únicos após filtragem. A ISI Web of Science revelou apenas 5 estudos únicos de um total de 25. A ScienceDirect começou com 73 estudos, restando 67 após a remoção de duplicatas. Na Scopus, 47 estudos foram encontrados, dos quais 16 eram únicos. Por fim, a Springerlink teve o maior número, com 620 estudos e 538 após a filtragem.

Após a importação, foram aplicados critérios de aceitação e exclusão, conforme apresentados na Tabela II, resultando em 766 estudos considerados aptos para revisão. Essa etapa é fundamental para garantir que apenas os estudos mais relevantes e alinhados ao objetivo da revisão sejam considerados para análise posterior. Desses, 164 foram analisados, levando à seleção final de 65 estudos relevantes. A distribuição dos estudos aceitos varia entre as bases, com a EI Compendex contribuindo com 19 estudos e a ACM Digital Library com 8.

TABELA II
CRITÉRIOS DE INCLUSÃO E EXCLUSÃO

Inclusão		
I1	Estudos em inglês	65
I2	Estudos publicados dentro do período de 2016 a 2023	

I3	Estudos que tratam da LGPD em engenharia de Requisitos	
I4	Estudos que tratam sobre a GDPR	
Exclusão		
E1	Estudos duplicados	182
E2	Estudos não disponíveis na íntegra	45
E3	Estudos publicados fora do período de 2016 a 2023	0
E4	Estudos que não tratam da GDPR	4
E5	Estudos que não tratam da LGPD	27
E6	Estudos que não tratam da engenharia de requisitos	37

IV. ANÁLISE E SÍNTESE DE RESULTADOS

Após as fases de planejamento e execução da RSL, procede-se à análise e síntese dos resultados obtidos, com o objetivo de apresentar as conclusões. Esta etapa foi desenvolvida com base em como os artigos lidos na fase de execução responderam, de modo geral, às questões de pesquisa definidas na etapa de planejamento da RSL. Para o desenvolvimento desta etapa, foram utilizados os 10 principais artigos obtidos em fases anteriores, uma vez que esses foram os que responderam de forma direta ou mencionaram conteúdos relevantes sobre as questões de pesquisa, os quais foram identificados através de atribuição de ID's, sendo eles, 3 [25], 4 [26], 5 [27], 9 [28], 24 [29], 29 [30], 30 [31], 32 [32], 48 [33], 62 [34].

A. Privacidade na LGPD e Engenharia de Requisitos

Esta seção tem como objetivo apresentar o conceito de privacidade dentro da LGPD e sua relação com o termo no contexto da Engenharia de Requisitos (ER). Ela visa responder à segunda questão de pesquisa (O que se entende por privacidade na LGPD e qual é sua relação com o termo privacidade na engenharia de requisitos?). Dentre as 64 evidências utilizadas, apenas 5 delas mencionam diretamente a definição do termo privacidade, conforme apresentado na Tabela III. No entanto, é importante destacar que o termo não possui uma definição única, não apenas no contexto da LGPD, mas também em um contexto geral. Portanto, sua definição é ambígua e diversificada, levando os autores a utilizarem diversas definições divergentes.

TABELA III
DEFINIÇÕES DE PRIVACIDADE EM CADA EVIDÊNCIA.

ID	Principais Conceitos Abordados
30	Definição de privacidade como um direito universal segundo a ONU.
29	Privacidade relacionada ao controle individual sobre informações na LGPD e na Engenharia de Requisitos (ER); Privacidade associada à identificação e definição de requisitos relacionados à proteção de dados na ER.
3	Privacidade relacionada ao controle individual sobre informações na LGPD.
9	Privacidade como conceito dinâmico, dependente de mudanças nas normas sociais e tecnológicas.
24	Enfatiza a importância de uma abordagem cuidadosa na gestão da privacidade para prevenir violações, destacando a falta de conhecimento, comportamentos descuidados e uso inadequado

da tecnologia como causas comuns de violações.

B. Abordagens da Engenharia de Requisitos para Conformidade com a LGPD

Nesta seção, aborda-se a primeira questão de pesquisa, "O que a engenharia de requisitos tem proposto para se adequar e entrar em conformidade com as exigências impostas pela LGPD?". Foram identificados 7 artigos que responderam a essa pergunta, com os seguintes ID's 3, 5, 9, 29, 30 e 48. Destaca-se que os artigos 5, 29 e 30 obtiveram nota máxima na avaliação de qualidade, indicando uma abordagem detalhada e abrangente sobre as estratégias da engenharia de requisitos para conformidade com a LGPD. A Tabela IV apresenta os artigos e suas propostas para entrar em conformidade com a LGPD.

TABELA IV
PROPOSTAS PARA ENTRAR EM CONFORMIDADE COM A LGPD

ID	Principais Propostas para Conformidade com a LGPD
3	Destaca o papel da Engenharia de Requisitos (ER) na prevenção de violações de privacidade, enfatizando a identificação precoce dos requisitos de privacidade. Linguagens de modelagem orientadas a objetivos, como i*2.0, NFR-Framework e Secure Tropos, são usadas para especificar requisitos de privacidade.
5	Menciona o uso do Inventário de Dados Pessoais (PDI) como uma prática para adequação às exigências da LGPD. O PDI identifica e documenta os dados pessoais coletados, processados e armazenados pelo sistema, garantindo transparência e gestão eficaz desses dados.
9	Profissionais da ER adaptam métodos clássicos para identificar e documentar os requisitos de privacidade, incluindo estudo de viabilidade, elicitação, análise, especificação e validação.
29	Propõe a identificação e a elicitação de requisitos de privacidade desde as fases iniciais do desenvolvimento de software.
30	Estuda diversas abordagens utilizadas por profissionais da ER para lidar com requisitos de privacidade, desde plug-ins para Ambientes de Desenvolvimento Integrado (IDEs) até metodologias sistemáticas.
48	Destaca o uso de frameworks, como o FLG framework, para modelagem automatizada de metas em regulamentações legais, como a LGPD.

C. Conformidade com LGPD na Engenharia de Requisitos

Nesta seção, serão exploradas a conformidade com a Lei Geral de Proteção de Dados (LGPD) e formas de alcançá-la. Desta forma, serão abordadas as questões de pesquisa três (Como garantir a conformidade com a LGPD na engenharia de requisitos?) e quatro (Existem soluções consolidadas para que os engenheiros de requisitos adaptem seu trabalho para estar em conformidade com a LGPD?).

A terceira questão aborda como a Engenharia de Requisitos (ER) se ajusta à LGPD. Como observado nas seções anteriores, muitos autores destacam a importância de priorizar a identificação e documentação dos requisitos de privacidade desde o início do processo de desenvolvimento de sistemas, visando a conformidade com a LGPD, conforme evidenciado no artigo de ID 29.

No entanto, conforme mencionado no trabalho de ID 9, as regulamentações frequentemente apresentam ambiguidades, o que torna desafiadora a extração e operacionalização desses requisitos. Por isso, vários autores ressaltam a necessidade de examinar a perspectiva dos profissionais de Tecnologia da Informação e Comunicação (TIC) em relação à privacidade, assim como a postura organizacional frente a essa questão, entre outros aspectos cruciais (citado no artigo de ID 9).

Atualmente, há uma lacuna evidente em relação à efetiva conformidade com a LGPD, mesmo com a presença da GDPR, devido à ausência de métodos consolidados para esse fim. Embora haja a abordagem clássica de documentação, conforme os procedimentos da ER, muitos profissionais a consideram cansativa e acabam por não utilizá-la. Diante desse cenário, diversos autores (conforme apresentado nos estudos de ID 's (4, 9, 62, 32, 30) têm se empenhado em desenvolver ferramentas, métodos e linguagens direcionadas para facilitar e auxiliar o processo de conformidade com a LGPD. Na próxima seção, serão apresentadas algumas dessas soluções.

D. Soluções para entrar em conformidade com a LGPD

Com o propósito de responder à quarta questão de pesquisa, esta subseção destacou soluções elaboradas no contexto da Engenharia de Requisitos (ER) para cumprir com a legislação de proteção de dados, a LGPD, a Tabela V apresenta as soluções propostas por cada um dos artigos citados, com o objetivo de alcançar conformidade com a LGPD. Como mencionado anteriormente, ainda não foram estabelecidas soluções completamente consolidadas para garantir a conformidade com essa legislação. Entretanto, nesse contexto, diversos autores têm desenvolvido várias técnicas com o intuito de apoiar e orientar os profissionais rumo à conformidade com a LGPD.

O conceito dos Princípios da Privacidade desde a concepção preconiza que a proteção dos dados pessoais deve ser considerada desde o início e ao longo de todo o ciclo de vida de qualquer projeto, sistema, serviço, produto ou processo. Segundo o Guia de Boas Práticas da LGPD, esse conceito é embasado em sete princípios fundamentais. Esses princípios incluem a abordagem proativa e preventiva, integrando a privacidade desde o design, garantindo segurança e proteção contínuas dos dados, bem como transparência e respeito pelos direitos dos usuários.

A privacidade por padrão e a funcionalidade total são igualmente enfatizadas, assegurando que a privacidade não seja uma reflexão tardia, mas sim um componente essencial e integral dos sistemas e processos organizacionais. A Engenharia de Privacidade é um campo emergente que veio à tona nos últimos anos lidando com o conceito de proteger a privacidade no campo de software e outras tecnologias emergentes. A engenharia de privacidade tem um papel mediano a nível sênior, lidando com a análise de restrições e aplicações de controle no design de softwares em ordem de garantir a privacidade através do design e privacidade por padrão ou para preencher as obrigações legais [35].

TABELA V

PROPOSTAS PARA ENTRAR EM CONFORMIDADE COM A LGPD

ID	Solução Proposta
4	LGPD for Business Process (LGPD4BP): Questionário para avaliar a conformidade dos processos com a LGPD, Catálogo de Padrões de Modelagem e método para modelar processos.
9	Utilização de Multiple Criteria Decision Analysis (MCDA) e Preference Ranking Organization Method for Enriched Evaluation (PROMETHEE) para priorizar iniciativas de segurança de dados.
62	RSLingo4Privacy: Especificação e análise de políticas de privacidade. RSL-IL4Privacy: Linguagem específica de domínio para representação precisa de requisitos de privacidade.
32	Princípios da Privacidade desde a Concepção (PbD) para consideração proativa da privacidade desde o início de um projeto.
30	Diversas abordagens, como Coconut, GuideMe, P-STORE, VIS-PRIZE, que oferecem métodos e técnicas para lidar com requisitos de privacidade no desenvolvimento de software.

E. Da GDPR à LGPD: Adaptação na Engenharia de Requisitos

Por fim, nesta seção será apresentada a resposta para a quinta e última questão de pesquisa (Como os trabalhos da engenharia de requisitos visando atender exigências de leis internacionais como a GDPR podem ser adaptados à realidade nacional?). O objetivo é discutir se as soluções desenvolvidas para a GDPR podem ser adaptadas para a legislação brasileira. Conforme mencionado anteriormente, a Lei Geral de Proteção de Dados (LGPD) foi inspirada no Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, o que resulta em diversas diretrizes semelhantes. No entanto, a LGPD possui 65 artigos, enquanto a GDPR possui 91 artigos, indicando diferenças entre eles.

Os autores do artigo de ID 48 destacam que os trabalhos da engenharia de requisitos voltados para atender às exigências de leis internacionais, como a GDPR, podem ser adaptados à realidade nacional por meio da identificação das semelhanças e diferenças entre as regulamentações. Essa adaptação envolve ajustar as práticas e processos de engenharia de requisitos para atender aos requisitos específicos de cada legislação nacional, como a LGPD no Brasil. Isso pode incluir a personalização de políticas, procedimentos e controles de segurança de acordo com as exigências locais, garantindo a conformidade com a legislação nacional de proteção de dados. A Tabela VI resume estas informações.

TABELA VI
ADAPTAÇÕES DE SOLUÇÕES DA GDPR PARA A LGPD.

ID	Solução Proposta
48	Destaca-se a viabilidade de adaptar as práticas da Engenharia de Requisitos da GDPR para atender às exigências da LGPD no Brasil, desde que as diferenças e semelhanças entre as leis sejam consideradas.

V. CONCLUSÃO

Desde a implementação do Regulamento Geral de Proteção de Dados (GDPR) em 2016, a proteção de dados ganhou relevância significativa em todo o mundo. No Brasil, esse movimento se refletiu na criação da Lei Geral de Proteção de Dados (LGPD), que entrou em vigor em 2018, impulsionando diversos aspectos no desenvolvimento de sistemas no contexto nacional. Nesse cenário, a privacidade emergiu como um tema central, destacando a importância crescente da Engenharia de Requisitos (ER) para garantir a conformidade dos sistemas com a legislação brasileira.

Esta Revisão Sistemática da Literatura (RSL) teve como objetivo identificar métodos, ferramentas, técnicas e processos empregados na Engenharia de Requisitos (ER) para atender às exigências da Lei Geral de Proteção de Dados (LGPD). Inicialmente, foram coletados 996 estudos de diversas bases de dados. Desses, 70 artigos foram selecionados como adequados para prosseguir como referência na presente RSL, utilizando os critérios de inclusão e exclusão definidos para filtragem. Após a leitura e aplicação dos critérios de avaliação, apenas 64 artigos obtiveram notas superiores a 0.0, sendo considerados para o desenvolvimento desta RSL.

Após a seleção dos estudos, realizou-se uma análise e síntese dos resultados, orientados pelas questões de pesquisa definidas anteriormente na fase de planejamento. Evidenciou-se que o conceito de privacidade, um dos temas centrais para a LGPD, carece de uma definição universal clara, o que dificulta sua compreensão devido à sua natureza ambígua e variada. No contexto da LGPD, a privacidade é abordada tanto diretamente quanto indiretamente em diversos artigos, tais como os artigos, Art. 1º, Art. 5º, Art. 6º, Art. 9º, Art. 18º, Art. 19º, Art. 20º, Art. 23º e Art. 46º. Esses artigos tratam de diferentes aspectos relacionados à proteção da privacidade dos indivíduos no contexto do tratamento de dados pessoais. A Tabela VII exemplifica como os artigos mencionados da LGPD tratam da questão da privacidade em suas disposições.

TABELA VII
PRIVACIDADE NA LGPD.

Artigo	Menção a privacidade
1º	Define o objetivo da Lei como a proteção da privacidade.
5º	As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: finalidade, adequação, necessidade, livre acesso, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas.
6º	Estabelece as bases legais para o tratamento de dados pessoais, incluindo o consentimento do titular dos dados e a proteção da privacidade como uma base legal.
9º	Trata do tratamento de dados pessoais sensíveis, relacionados diretamente à privacidade das pessoas.
18º	Garante o direito à confirmação da existência de tratamento de dados pessoais e o acesso aos dados, fundamentais para o exercício do controle sobre a

	privacidade.
19º	Confere ao titular dos dados o direito de correção de dados incompletos, inexatos ou desatualizados, contribuindo para garantir a precisão das informações pessoais e, conseqüentemente, a proteção da privacidade.
20º	Assegura o direito à eliminação dos dados pessoais tratados com o consentimento do titular, relacionado ao controle sobre as informações pessoais e à privacidade.
23º	Estabelece princípios para o tratamento de dados pessoais, incluindo a finalidade, a adequação, a necessidade e a minimização dos dados, visando proteger a privacidade dos titulares.
46º	Trata das transferências internacionais de dados pessoais, considerando também a privacidade dos titulares dos dados em contextos transfronteiriços.

Além disso, foi observado que no âmbito da Engenharia de Requisitos (ER) existem diversas soluções voltadas para auxiliar os profissionais a mapear requisitos visando garantir a conformidade com a LGPD, conforme apresentado na Tabela VII. Embora não haja uma solução única e definitiva, foram desenvolvidas diversas abordagens, como a LGPD4BP, um questionário para avaliar a conformidade dos sistemas com a LGPD. Os autores não exploram no estudo sobre quais artigos da LGPD a abordagem foi definida, entretanto, a LGPD4BP é fundamentada nos artigos da LGPD que tratam da proteção de dados pessoais e das obrigações das organizações em relação ao tratamento desses dados, como o Art. 5º.

Além disso, também foi constatado que métodos originalmente concebidos para a GDPR podem ser adaptados para o contexto nacional, desde que sejam identificadas as semelhanças e diferenças entre as regulamentações. Além da utilização de métodos já estabelecidos na Engenharia de Requisitos, como a i*2.0 e o NFR-Framework (*Non-functional Requirements Framework*), estão sendo empregados para a especificação precoce de requisitos de privacidade, uma vez que são referências reconhecidas para a identificação de requisitos não funcionais.

Desta forma, a presente RSL revelou lacunas significativas relacionadas à efetiva conformidade com a LGPD. A área ainda apresenta várias questões não resolvidas, como a definição do termo "privacidade", que carece de uma definição única e universal, deixando assim a interpretação a critério dos profissionais de ER, entre as várias disponíveis. Além disso, foram identificadas diversas ferramentas que podem ser utilizadas para alcançar a conformidade com a LGPD, porém nenhuma delas se encontra consolidada até o momento. Portanto, são os próprios autores do campo que estão encarregados de desenvolver métodos para auxiliar os profissionais nessa tarefa.

Embora as metodologias clássicas da ER também sejam utilizadas, muitos profissionais ainda as consideram cansativas e acabam por não adotá-las plenamente. Assim, ainda é necessário realizar estudos adicionais para desenvolver métodos que sejam consolidados e eficazes para garantir a conformidade com a LGPD.

Assim, a Engenharia de Requisitos (ER) demonstrou sua importância no desenvolvimento de sistemas, especialmente devido ao seu papel crucial na gestão dos requisitos de privacidade. Embora ainda haja lacunas em soluções consolidadas e ágeis para a conformidade com a LGPD, os avanços nessa área são promissores e indicam uma evolução contínua na adaptação dos sistemas às exigências legais de proteção de dados.

REFERÊNCIAS

- [1] União Europeia, "Regulamento Geral de Proteção de Dados," Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679>.
- [2] SEBRAE, "Lei Geral de Proteção de Dados (LGPD)," 2021. Acesso em 30 de janeiro de 2023. Disponível em: https://sebrae.com.br/sites/PortalSebrae/canal_adicionais/conheca_lgpd.
- [3] BRASIL, "Lei Geral de Proteção de Dados Pessoais (LGPD), 2018. Acesso em 30 de janeiro de 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm.
- [4] KOTONYA, G.; SOMMERVILLE, I. *Requirements Engineering: Processes and Techniques*. Chichester: John Wiley & Sons, 1998.
- [5] SOMMERVILLE, I. *Engenharia de Software*. 9. ed. [S.l.]: Pearson Education, 2011.
- [6] CHUNG, L.; LEITE, J. C. S. d. P. On non-functional requirements in software engineering. *Journal of Systems and Software*, January 2009. DOI: 10.1016/j.jss.2008.03.051.
- [7] BUCCI, M. P. D. *Fundamentos para uma teoria jurídica das políticas públicas*. 2. ed. São Paulo: Saraiva Educação, 2021.
- [8] GOMES, C. *Scrum: A Metodologia Ágil Simplificada*. 2017. Acesso em 30 de janeiro de 2023. Disponível em: <https://blog.europneumaq.com/scrum-metodologia-agil-simplificada>.
- [9] NAKAGAWA, E. et al. Revisão sistemática da literatura em engenharia de software. In: . S.l.: Elsevier Editora Ltda, 2017a. cap. Questão 2: Qual a origem da RS?
- [10] SACKETT, D. L.; AL. et. Evidence based medicine: what it is and what it isn't. *BMJ*, janeiro 1996. Disponível em: <https://www.bmj.com/lookup/doi/10.1136/bmj.312.7023.71>.
- [11] KITCHENHAM, B. *Procedures for Performing Systematic Reviews*. [S.l.], 2004.
- [12] NAKAGAWA, E. et al. Revisão sistemática da literatura em engenharia de software. In: . S.l.: Elsevier Editora Ltda, 2017b. cap. Questão 3: Como conduzir uma RS e

quais são as diretrizes existentes?

- [13] NUNES, C. A. R. o. Anais de Artigos Completos do VII CIDHCoimbra 2022 - Volume 10. Campinas/Jundiaí: Brasília/Edições Brasil, 2023. 402 p. (Série Simpósios do VII CIDHCoimbra 2022).
- [14] DEFENSORIA PÚBLICA DO ESTADO DO RIO GRANDE DO SUL. Entendendo a Lei Geral de Proteção de Dados. 1.0. ed. [S.l.], 2021. Acesso em 23 jan 2024.
- [15] GOVERNO FEDERAL DO BRASIL. Guia de Boas Práticas Lei Geral de Proteção de Dados (LGPD). 2020. Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf>.
- [16] PINHEIRO, P. P. Proteção de Dados Pessoais: Comentários à Lei n. 13.709/2018 - LGPD. 2. ed. [S.l.: s.n.], 2020.
- [17] SENADO, A. Punições pelo uso indevido de dados pessoais começam a valer no domingo. 2021.
- [18] GOVERNO FEDERAL DO BRASIL. ANPD aplica a primeira multa por descumprimento à LGPD. 2023. Acesso em 23 janeiro de 2024. Disponível em: <<https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-aplica-a-primeira-multa-por-descumprimento-a-lgpd>>.
- [19] VALENTE, M. T. Engenharia de Software Moderna. 1ª. ed. Editora Independente, 2022. Acesso em 22 jan 2024. Disponível em: <<https://engsoftmoderna.info>>.
- [20] BECKERS, C. Comparing privacy requirements engineering. 2012. Disponível: <<https://ieeexplore.ieee.org/document/6329233>>.
- [21] ANSARI, M. T. J. et al. P-STORE: Extension of STORE Methodology to Elicit Privacy Requirements. *Arabian Journal for Science and Engineering*, 2021.
- [22] PASSOS, M. Parte 2: Da teoria da privacidade à prática de engenharia. 2022. Disponível em: <<https://dponapratica.com.br/2022/07/parte-2-da-teoria-da-privacidade-a-pratica-de-engenharia/>>.
- [23] PARSIFAL. Parsifal. 2024. Acesso em 18 jan 2024. Disponível em: <<https://parsif.al/>>
- [24] KITCHENHAM, B.; CHARTERS, S. *Guidelines for performing Systematic Literature Reviews in Software Engineering*. [S.l.], 2007. v. 2.3, n. EBSE-2007-01.
- [25] M. M. Peixoto and C. Silva, “Specifying Privacy Requirements with Goal-Oriented Modeling Languages,” 2018. ACM Digital Library.
- [26] E. Araújo, J. Vilela, C. Silva, and C. Alves, “Are My Business Process Models Compliant With LGPD? The LGPD4BP Method to Evaluate and to Model LGPD Aware Business Processes,” 2021. ACM Digital Library.
- [27] J. Saraiva and S. Soares, “Adoption of the LGPD Inventory in the User Stories and BDD Scenarios Creation,” 2023. ACM Digital Library.
- [28] E. D. Canedo, A. T. S. Calazans, I. N. Bandeira, P. H. T. Costa, and E. T. S. Masson, “Guidelines adopted by agile teams in privacy requirements elicitation after the Brazilian general data protection law (LGPD) implementation,” 2022. El Compendex.
- [29] T. Mäesalu and K. Mooses, “The Benefits of Agent-Oriented Goal Model in Developing Data Protection Application for Lecturers,” 2023. Springer Link.
- [30] E. D. Canedo, A. T. Seidel Calazans, A. J. Cerqueira, P. H. T. Costa, and E. T. Masson, “Agile Teams’ Perception in Privacy Requirements Elicitation: LGPD’s compliance in Brazil,” 2021. El Compendex.
- [31] P. H. Da Silva, F. B. Vavassori Benitti, and M. S. Wangham, “How Has Requirements Engineering Supported Data Protection?” 2022. El Compendex.
- [32] Y. S. Martin and A. Kung, “Methods and Tools for GDPR Compliance through Privacy and Data Protection Engineering,” 2018. ISI Web of Science.
- [33] A. Rabinia and S. Ghanavati, “The FOL-based legal-GRL (FLG) framework: Towards an automated goal modeling approach for regulations,” 2018. Scopus.
- [34] J. Caramujo, A. R. da Silva, S. Monfared, A. Ribeiro, P. Calado, and T. Breaux, “RSL-IL4Privacy: a domain-specific language for the rigorous specification of privacy policies,” 2018. Springer Link.
- [35] UNDERWOOD, C. What Is Privacy Engineering? 2023. Disponível: <<https://cunderwood.dev/2023/01/08/what-is-privacy-engineering/>>