Universidade de Brasília

Instituto de Ciências Exatas
Departamento de Ciência da Computação

Análise Comparativa de Leis de Proteção de Dados e Frameworks de Privacidade: Otimizando Soluções para Conformidade com LGPD e Leis Internacionais de Compartilhamento de Dados

Lucas Dalle Rocha

Dissertação apresentada como requisito parcial para
conclusão do Mestrado em Informática

Orientadora
Prof.a Dr.a Edna Dias Canedo

Brasília
2024

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

Análise Comparativa de Leis de Proteção de Dados e Frameworks de Privacidade: Otimizando Soluções para Conformidade com LGPD e Leis Internacionais de Compartilhamento de Dados

Lucas Dalle Rocha

Dissertação apresentada como requisito parcial para
conclusão do Mestrado em Informática

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

Prof.a Dr.a Carla Taciana Lima Lourenço Silva Schuenemann
CIN/UFPE

Prof.a Dr.a Genaina Nunes Rodrigues
CIC/UnB

Prof. Dr. Rodrigo Bonifácio de Almeida
Coordenador do Programa de Pós-graduação em Informática

Brasília, 18 de novembro de 2024

Dedicatória

A todos aqueles que, independentemente das circunstâncias, demonstram uma constante e indomável disposição para o aprendizado.

Agradecimentos

Em primeiro lugar, gostaria de agradecer aos meus pais, William e Christiana, por me fazerem acreditar que eu posso atingir qualquer objetivo desde que eu tenha vontade e dedicação. Eles são os meus exemplos de dedicação e me motivam a ser a melhor versão de mim.

Em segundo, gostaria de agradecer à minha companheira, Beatriz, pelo amor e carinho mesmo com as dificuldades proporcionadas pelo longo período de dedicação ao trabalho. Você nunca deixou de sorrir pra mim e de me motivar, por isso sou muito grato.

E por fim, mas não menos importante, quero prestar meus agradecimentos à orientadora Prof. Edna Dias Canedo, que tornou todo esse trabalho possível. Sem o seu auxílio, paciência e expertise, esse trabalho não seria possível.

Resumo

Contexto: No cenário atual de globalização e interconectividade, organizações e desenvolvedores enfrentam um desafio complexo para garantir a conformidade com as diversas leis de privacidade do mundo. Com a troca de dados transfronteiriça sendo uma prática comum, não basta estar em conformidade apenas com a legislação local, que é a Lei Geral de Proteção de Dados (LGPD) no Brasil, mas é preciso entender e cumprir o máximo possível de regulamentações internacionais para garantir a proteção e a privacidade de dados dos usuários e evitar sanções administrativas. **Objetivo:** O objetivo principal deste trabalho é construir um guia abrangente para auxiliar organizações e desenvolvedores a alcançarem a conformidade com várias leis de privacidade, incluindo a LGPD, *General Data Protection Regulation* (GDPR), *American Data Privacy and Protection Act* (ADPPA) e *Australian Privacy Act*, a partir de dois frameworks de privacidade, Privacy by Design e ISO/IEC 29100. Dessa forma, são catalogadas semelhanças e diferenças das diretrizes, a fim de que a implementação em software seja unificada por meio dos frameworks, além dos desafios apontados pelos desenvolvedores e suas organizações no processo de conformidade com as legislações. **Método:** Realizamos uma Revisão Sistemática de Literatura (RSL) para identificar os pontos de convergência e divergência entre as leis de privacidade de dados, bem como as dificuldades das organizações em aplicá-las. Os pontos identificados foram inseridos em um quadro comparativo por meio de análise qualitativa da RSL e os desafios foram categorizados e codificados. Quanto aos desafios, foi realizado um *survey* para validá-los em um contexto brasileiro e, a partir de teoria fundamentada, reformular a categorização dessas dificuldades. Já para as comparações das leis, foi aplicado o método de Framework Analysis, que permite a codificação e indexação dos principais pontos das legislações, a fim de correlacioná-los com os frameworks estudados e propor a ferramenta que auxiliará as organizações no processo de conformidade. **Resultados:** A pesquisa revelou que a maior dificuldade das organizações e dos desenvolvedores reside na escassez de conhecimento sobre as leis, tanto teórico quanto prático. Assim, ainda que as legislações sejam parecidas em diversos pontos (como LGPD e GDPR), os desenvolvedores não as compreende em sua completude e apresentam desafios quanto à tradução da lei para um contexto técnico, que é presente desde a etapa de elicitação de

requisitos. **Conclusão:** Essa pesquisa contribui para a compreensão mais clara das implicações das leis de privacidade de dados em um contexto globalizado e oferece orientações práticas aos profissionais de TIC para lidar com os desafios associados à conformidade com essas regulamentações.

Palavras-chave: Privacidade de Dados, Requisitos de Privacidade, Desafios de Privacidade, Lei Geral de Proteção de Dados Pessoais, ISO/IEC 29100, Frameworks de Privacidade

Abstract

Context: In the current scenario of globalization and interconnectedness, organizations and developers face the complex challenge of ensuring compliance with multiple privacy laws. With cross-border data exchange being a common practice, it is not enough to comply solely with local legislation, such as the General Data Protection Law (LGPD) in Brazil, but it is necessary to understand and comply with as many international regulations as possible to ensure the protection and privacy of user data and avoid administrative sanctions. **Objective:** In this study, we aim to construct a comprehensive guide to aid organizations and developers in achieving compliance with multiple privacy laws, including LGPD, the General Data Protection Regulation (GDPR), the American Data Privacy and Protection Act (ADPPA), and the Australian Privacy Act, alongside two renowned privacy frameworks, Privacy by Design and ISO/IEC 29100. In this way, similarities and differences between the guidelines are catalogued, so that software implementation can be unified through the frameworks, as well as the challenges pointed out by developers and their organizations in the process of complying with the legislation. **Method:** Initially, a Systematic Literature Review (SLR) was conducted to identify points of convergence and divergence between the laws, as well as the difficulties organizations face in applying them. Relevant topics were inserted into a comparative framework through qualitative analysis of the SLR, and challenges were categorized and coded. Regarding the challenges, a survey was conducted to validate them in a Brazilian context and, based on grounded theory, reformulate the categorization of these difficulties. As for the comparisons of the laws, the Framework Analysis method was applied, which allows coding and indexing of the main points of the legislations to correlate them with the studied frameworks and propose the tool that aids organizations in the compliance process. **Results:** The research revealed that the greatest difficulty for organizations and developers lies in the scarcity of knowledge about the laws, both theoretically and practically. This means that, even though the legislations are similar in many points (such as LGPD and GDPR), developers do not fully understand them and face challenges in translating the law into a technical context, which is present from the requirements elicitation stage. **Conclusion:** This dissertation contributes to a clearer understanding of the implications of privacy laws in

a globalized context and offers practical guidance to deal with the challenges associated with compliance with these complex regulations.

Keywords: Data Privacy, Privacy Requirements, Privacy Challenges, General Data Protection Law, Privacy by Design, ISO/IEC 29100, Privacy Frameworks

Sumário

Lista de Figuras

Lista de Tabelas

Capítulo 1

Introdução

Desde o período anterior à Indústria 4.0, o avanço tecnológico corrobora progressivamente com a migração de dados do meio físico para o meio digital, de modo que uma quantidade massiva de informações é diariamente armazenada em servidores locais e em nuvem [1]. Em meio organizacional, a capacidade de tratamento eficiente — como o compartilhamento e armazenamento dessas informações — está intimamente relacionada ao fator microeconômico, de modo a validar o interesse na digitalização da maior parte dos dados [1]. Nos dias atuais, a vasta aplicabilidade de software permite a distribuição de múltiplos tipos de dados pessoais, que vai desde informações tratadas em meio puramente econômico [2], até aquela que ocorre em âmbitos educacional e profissional, mais recentemente por meio da digitalização forçada proporcionada pela pandemia do vírus COVID-19 [3]. Essa vertiginosa migração digital levanta questões a respeito do compartilhamento internacional e da privacidade dos dados pessoais [4].

Em um ambiente digital, é habitual a ampla transferência de arquivos que contêm dados armazenados em sua estrutura — os denominados metadados —, como textos, imagens, vídeos, etc., uma vez que ocupam apenas um pequeno espaço em memória relativo ao conteúdo armazenado [5], fato que corrobora para a intensificação do meio digital em oposição ao físico. Todavia, uma vez que há enfoque no massivo compartilhamento desses arquivos, em meio ao contexto de Big Data, é necessário resguardar a privacidade dos envolvidos e, habitualmente, o objetivo é atingido por meio de legislações locais que visam a proteção dos dados pessoais [6], [7].

No âmbito organizacional, o armazenamento ineficaz de documentos digitais por parte de organizações brasileiras proporcionou, em apenas um ano, o vazamento de mais de duzentos milhões de dados pessoais [8]. Além do tratamento inadequado dos dados pessoais — que viola o direito de privacidade dos envolvidos em caso de vazamento —, os arquivos, em sua maioria, não costumam ser sanitizados, isto é, tratados para que seus metadados não possam ser revelados por atacantes [9]. Dessa forma, a negligência em

tratar adequadamente tais documentos afeta não só os indivíduos diretamente envolvidos — de modo a revelar seus dados pessoais —, como também a organização responsável, visto que os metadados expostos revelam informações cruciais acerca do armazenamento dos documentos.

Assim, a proteção dos dados pessoais apresenta-se como uma abordagem essencial para resguardar a privacidade dos envolvidos, uma vez que a sua escassez permite relacionar as informações expostas à uma pessoa exclusiva, isto é, torná-la identificável [6], [10]. Deve-se, portanto, evitar a identificação de um indivíduo através de seus dados pessoais sensíveis, por meio de diversas técnicas que variam conforme o tipo (sensível ou não), forma, impacto, etc. [6], [11].

Já no âmbito legal, a Lei Geral de Proteção de Dados (LGPD) — Lei n° 13.709 —, decretada no dia 14 de agosto de 2018, conceitua um dado pessoal e aborda uma série de princípios a serem seguidos, a fim de garantir a privacidade individual [12]. No Art. 3°, há manifestação da extraterritorialidade da lei [12] e isso significa que empresas multinacionais, mesmo que atuem fora do território nacional, são requisitadas à adoção dos princípios da LGPD, caso processem dados de brasileiros naturais. Todavia, os princípios apresentados no Art. 6° tratam-se de uma generalização que busca atingir toda a população de maneira proporcional (inclusive as organizações responsáveis pelo tratamento dos dados), ou seja, uma abstração pouco técnica observada em múltiplas leis de privacidade pelo mundo [13]. Dito isso, empresas devem recorrer aos guias ou às metodologias avulsas a fim de colocar em prática a privacidade e quase nunca há um consenso quando se trata de dados internacionais e múltiplas legislações [13], [4], [14].

Nesse contexto, o tratamento dos dados pessoais, que vão desde a coleta até a eliminação dos dados, deverá estar em conformidade com o Art. 6° da LGPD [12], haja enfoque nas etapas de compartilhamento e armazenamento dos dados via documentos digitais. Dessa forma, uma vez que os princípios sejam aplicados relativos a cada dado pessoal crítico, haverá possibilidade de minimização de riscos em caso de vazamento. Logo, os responsáveis pelo tratamento dos dados deverão, em síntese, estar a par dos princípios e direitos da LGPD e, além disso, de técnicas que garantam a proteção dos dados e quando utilizá-las.

Além disso, como supracitado, o oposto também deve ser considerado, isto é, organizações que atuam em território brasileiro devem levar em conta que habitualmente lidarão com dados internacionais, resguardados por legislações externas. Logo, não basta estar em conformidade apenas com a lei nacional ou regional de privacidade, mas é essencial conhecer as leis comumente praticadas e solucionar, quando conveniente, os dilemas entre as mesmas [15].

A partir disso, ao alcançar os direitos de liberdade e privacidade dos dados, que se almeja no Art. 1°, *caput* da lei [12], há garantia por parte dos responsáveis pelo tratamento dos dados de que, caso ocorra uma violação das informações armazenadas pela organização, a mesma não se encontrará vulnerável. Dito isso, é importante elucidar técnicas para se alcançar a conformidade com os princípios da LGPD já validadas anteriormente e, a partir disso, quantificar e selecionar as aplicações ideais para cada tipo de dado pessoal.

1.1 Problema de Pesquisa

Diante da crescente digitalização e compartilhamento de documentos, alguns responsáveis envolvidos no tratamento dos dados ainda não sabem como traduzir a lei para um contexto técnico por variadas razões [13], [16], [4], [17], [18], ou seja, não apresenta conhecer em completude quais métodos deverão ser utilizados para garantir a conformidade com os princípios da Lei Geral de Proteção de Dados (LGPD) [18]. Ademais, além de compreender os termos relevantes da legislação nacional (definições) e suas possíveis aplicações práticas, é indispensável conhecer também as legislações de privacidade de outros países, uma vez que elas podem ser aplicadas no contexto do compartilhamento internacional de dados, garantindo, assim, o tratamento adequado a usuários estrangeiros [4].

Dessa forma, este trabalho investigará as nuances entre as leis de privacidade de dados e frameworks utilizados em diversos países, por meio de uma comparação com a LGPD, ao mesmo tempo em que busca unificar soluções para os desafios enfrentados por organizações e desenvolvedores na criação de um ambiente digital que respeite a privacidade dos usuários. Para isso, foram realizados um levantamento sistemático de literatura e um survey, que validou os desafios enfrentados pelos desenvolvedores brasileiros e serviu de base para a elaboração do guia proposto. Posteriormente, outro survey foi conduzido para validar o guia desenvolvido.

1.2 Justificativa

Dada a rápida migração de informações para o ambiente virtual [19], a exposição de dados pessoais tornou-se uma questão relevante, uma vez que violações de privacidade vão de encontro ao explicitado pela Lei Geral de Proteção de Dados (LGPD) [12], que reforçou a necessidade de salvaguardar essas informações. Contudo, a conformidade com a legislação local não é suficiente, considerando que algumas leis possuem escopo extraterritorial [20]. Assim, é essencial que organizações apliquem tecnicamente múltiplas legislações de privacidade, de forma a considerar a nacionalidade e outros atributos dos titulares dos

dados [21], a fim de contornar o problema do compartilhamento internacional de dados [4], [18], [22].

É nesse cenário multifacetado que surge a importância de frameworks de privacidade, como o Privacy by Design e o ISO/IEC 29100, que oferecem diretrizes fundamentais para a implementação de privacidade em software [23]. Esses frameworks fornecem às organizações ferramentas práticas para integrar a privacidade desde as etapas iniciais do desenvolvimento, a fim de contribuir para a conformidade com legislações diversas — desde que utilizados em conjunto das respectivas leis [24] — e para a proteção efetiva de dados pessoais.

Além disso, os desafios enfrentados pelos desenvolvedores e suas respectivas organizações, especialmente em relação à elicitação de requisitos e às soluções técnicas, demandam diretrizes claras e práticas que incorporem os princípios de privacidade às etapas do desenvolvimento de software [25]. Essa abordagem promove soluções unificadas e eficazes para a proteção de dados em um contexto cada vez mais globalizado.

1.3 Objetivos

1.3.1 Objetivo Geral

O objetivo geral deste estudo é desenvolver um conjunto de informações que oriente desenvolvedores e suas respectivas organizações na escolha dos frameworks de privacidade mais adequados para enfrentar desafios específicos e assegurar a conformidade com as leis de proteção de dados, como a LGPD. Para isso, a pesquisa explora similaridades e diferenças entre as legislações de proteção de dados no Brasil, União Europeia, Estados Unidos e Austrália, e analisa como frameworks de privacidade, como o ISO/IEC 29100 e o Privacy by Design, podem ser associados às leis para apoiar a implementação de normas de proteção de dados pessoais.

1.3.2 Objetivos Específicos

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

1. Realizar um estudo comparativo para identificar as similaridades e diferenças entre as leis de proteção de dados do Brasil, União Europeia, Estados Unidos e Austrália;

2. Investigar a conformidade na percepção dos desenvolvedores e organizações com a Lei Geral de Proteção de Dados (LGPD);

3. Analisar a conformidade identificada com relevantes padrões conhecidos e utilizados, como ISO/IEC 29100–*Information technology–Security techniques–Privacy* framework e Privacy by Design;

4. Catalogar as técnicas utilizadas na literatura e na indústria e os desafios enfrentados pelos membros das equipes e organizações para alcançar a conformidade;

5. Propor um guia para apoiar a garantia da conformidade com as leis de privacidade.

6. Verificar e validar o guia proposto e realizar ajustes, caso necessário.

1.4 Resultados Esperados

Ao final deste trabalho será disponibilizado um catálogo que apresenta as principais similaridades e diferenças entre as leis de privacidade de dados analisadas nesta pesquisa. Esse catálogo servirá como uma ferramenta de referência para profissionais que precisam compreender rapidamente as variações entre as legislações, facilitando decisões estratégicas em conformidade com diferentes requisitos legais. Além disso, será elaborado um guia prático para apoiar os profissionais envolvidos no tratamento dos dados pessoais, oferecendo orientações sobre como correlacionar os frameworks com as leis e garantir a conformidade com a Lei Geral de Proteção de Dados (LGPD) e outras legislações relevantes.

1.5 Metodologia de Pesquisa

A metodologia adotada na condução do trabalho é o método comparativo monográfico, que visa identificar semelhanças e diferenças entre as legislações vigentes, de modo aprofundado [26]. Por meio do framework analysis, é feita a leitura de todas as leis e categorização de aspectos relevantes, bem como a indexação de cada informação para cada diretriz e, posteriormente, a comparação [27]. Além disso, utiliza-se da pesquisa exploratória — que integra o levantamento bibliográfico acerca da comparação das legislações e dos frameworks, além da identificação dos desafios das organizações e dos profissionais da área (Revisão Sistemática de Literatura) — e explicativa, por meio da utilização de *survey* para a coleta de informações em relação às dificuldades encontradas pelos profissionais brasileiros e possíveis soluções para elas. A revisão é embasada também na técnica de snowball, a fim de identificar trabalhos relevantes entre si e especializar quanto às questões de pesquisa [28]. Por fim, a análise das respostas dos questionários foi feita por meio de uma abordagem qualitativa — com ênfase na teoria fundamentada [29] —, com o intuito de inferir os desafios e soluções relacionados à multiplicidade de legislações nas

organizações. A Figura 1.1 aponta as etapas envolvidas no processo da metodologia para o desenvolvimento do trabalho.

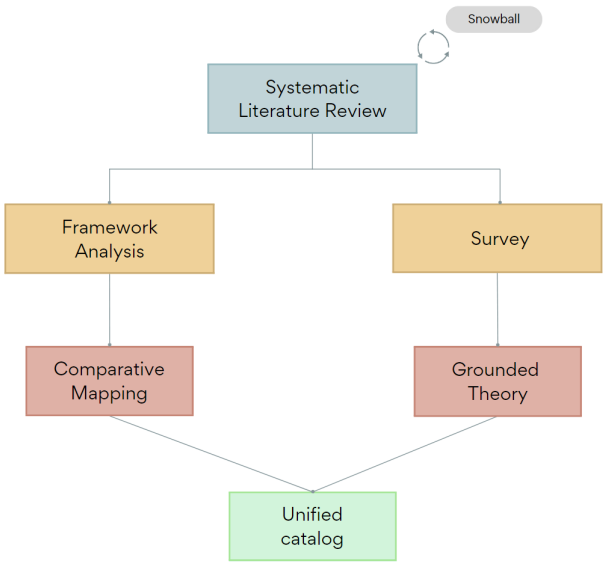


Figura 1.1: Etapas para realização da pesquisa.

Dessa forma, para a descrição completa do processo metodológico e, a partir da Figura 1.1, têm-se a seguinte sequência de etapas:

1. Revisão das leis de privacidade vigentes (brasileira, europeia, norte-americana e australiana) — Revisão Sistemática de Literatura;
2. Revisão de frameworks de privacidade (ISO/IEC 29100 e Privacy by Design) — Revisão Sistemática de Literatura;
3. Investigação e relação dos trabalhos correlatos — Revisão Sistemática de Literatura;
4. Questionamento acerca das principais similaridades e diferenças das diretrizes — Revisão Sistemática de Literatura;
5. Questionamento acerca dos principais desafios dos profissionais e organizações ao lidar com múltiplas legislações — Revisão Sistemática de Literatura;
6. Realização de um questionário para identificar os desafios enfrentados pelos profissionais brasileiros ao lidar com dados transfronteiriços — Survey;
7. Análise dos resultados identificados — Teoria Fundamentada;
8. Aplicação do método de framework analysis em conjunto com as informações obtidas na Revisão Sistemática de Literatura para realizar o processo de análise comparativa das legislações e frameworks — Framework Analysis e Mapeamento Comparativo;

9. Proposição de um guia simplificado e embasado nos frameworks para unificação das diretrizes propostas — Catálogo Unificado;

10. Verificação e Validação do guia proposto e realização de ajustes, caso necessário — Catálogo Unificado.

1.6 Estrutura do Trabalho

Este trabalho está organizado da seguinte maneira: o Capítulo 2 apresenta o referencial teórico que contempla as áreas importantes relacionadas aos objetivos específicos, e que são necessárias para compreensão do trabalho. Dessa forma, há abordagem de aspectos significativos das legislações de privacidade — a Lei Geral de Proteção de Dados, o Regulamento Geral de Proteção de Dados, a Lei Americana de Proteção à Privacidade de Dados e a Lei de Privacidade Australiana —, bem como o escopo, as definições, os direitos individuais e os princípios, além de elucidar princípios dos frameworks *Privacy by Design* e ISO/IEC 29100.

O Capítulo 3 apresenta a Revisão Sistemática de Literatura (RSL), em que há descrição do protocolo e os resultados, isto é, o comparativo das legislações e frameworks propostos e os desafios das organizações identificados na RSL ao se adequar às múltiplas legislações.

O Capítulo 4 apresenta a aplicação do questionário para desenvolvedores brasileiros que busca validar os desafios encontrados na RSL, isto é, se há compatibilidade entre as dificuldades descritas e as soluções apresentadas no guia.

O Capítulo 5 aborda a conversão dos resultados da RSL no mapeamento e no guia proposto, ou seja, o guia em sua versão inicial.

O Capítulo 6 propõe a Verificação e Validação do guia e os ajustes necessários para a proposição da versão final, além das implicações e contribuições em relação aos resultados do trabalho.

O Capítulo 7 expõe as contribuições teóricas do estudo com relação aos trabalhos relacionados, haja vista os resultados obtidos, além de elucidar preocupações futuras.

O Capítulo 8 apresenta uma síntese da contribuição do trabalho no âmbito de desenvolvimento e dos resultados alcançados, além de trabalhos futuros como motivação para novos objetos de estudo.

Capítulo 2

Contextualização

Neste capítulo serão apresentados os conceitos necessários para o entendimento deste trabalho.

2.1 Legislações de Privacidade de Dados

2.1.1 Lei Geral de Proteção de Dados Pessoais

A regulamentação brasileira que elucida o dever de tratamento adequado dos dados pessoais por responsáveis, dadas as condições, é a Lei Geral de Proteção de Dados Pessoais (LGPD) – Lei n° 13.709 [12]. Em vigência desde agosto de 2020, a lei busca garantir, em seu escopo de aplicação territorial, a idoneidade da privacidade de dados para toda a população brasileira, ainda que o processamento não seja efetuado em território nacional, desde que a coleta ocorra [18]. Isso significa que, em um mundo cada vez mais interconectado — em que aplicações tratam dados pessoais provenientes de diferentes nacionalidades —, para garantir a proteção dos dados é imprescindível conhecer as respectivas legislações de privacidade locais, bem como suas semelhanças e diferenças [30],[31]. Dito isso, é importante elucidar os principais conceitos da LGPD, bem como suas entidades envolvidas.

Inicialmente, é primordial entender como os dados são divididos e entendidos pela lei, uma vez que o processo de anonimização é, em sua forma rudimentar, uma conversão entre esses tipos de dados. A lei define, no Art. 5° (I-III), três tipos de dados e seus seguintes conceitos, além de estabelecer no Art. 5° (IX) o conceito de anonimização e de definir o órgão responsável pela garantia da LGPD em território nacional, vide Art. 5° (XIX) [12]:

I. dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

II. dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

III. dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

IX. anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

Em relação às entidades envolvidas, a LGPD define no Art. 5° (VI-VIII) as entidades envolvidas no processo de tratamento dos dados pessoais e, no Art. 5° (XIX), é definido o órgão regulatório que garante a conformidade dos envolvidos com a LGPD em território nacional [12]:

VI. controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

VII. operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

VIII. encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

XIX. autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

Dessa forma, entende-se que o dado pessoal é uma informação que tem a capacidade de identificar uma pessoa, a partir do mesmo. O grande impasse é que não é incomum a ocorrência de vazamento de dados em organizações — inclusive as renomadas —, logo um dado pessoal vazado igualmente apresenta uma elevada capacidade de exposição de um indivíduo [32]. A situação é ainda pior ao se tratar de uma violação ao dado pessoal sensível, uma vez que esse tipo de dado tem um caráter de vulnerabilização do indivíduo, isto é, o potencial de acarretar em discriminação [33], caso seja identificado. A evidente solução para organizações seria, então, realizar a anonimização de ambos tipos de dados (que são resguardados pela LGPD) a fim de torná-los dados anonimizados [19]. A Figura

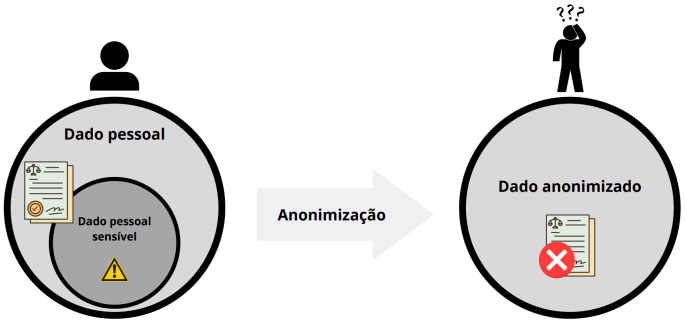


Figura 2.1: Diagrama de tipos de dados da LGPD [12].

2.1 demonstra a relação entre esses tipos de dados, a fim de esquematizar a base legal para o processo de anonimização.

Vale ressaltar que uma vez que os dados estão anonimizados, os mesmos não são mais legalmente abarcados pela LGPD, como evidencia a Figura 2.1. É o mesmo que dizer que os responsáveis pelo tratamento dos dados possuem respaldo legal para operar sobre essas informações sem que as sanções sejam aplicadas em caso de não conformidade, visto que não mais se trata de dados pessoais.

De acordo com Doneda [34], o processo de anonimização visa meramente a redução de riscos e é trivial perceber que tal técnica garante a segurança do usuário em meio digital. Além disso, por um viés econômico, pode ser considerada uma importante vantagem competitiva para empresas por dois motivos: ao reduzir a possibilidade de violações de dados pessoais, há uma priorização da reputação, ou seja, motiva a captação de novos clientes e mantém o interesse dos habituais; e, por estar em conformidade com leis vigentes de privacidade, inviabiliza a aplicação de sanções por não estar em conformidade [35]. Todavia, existe uma clara exceção no Art. 12°, ao evidenciar que [12]:

> "Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido."

O conceito de anonimização apresentado pela lei, ao buscar certa atemporalidade em exigir "meios técnicos razoáveis e disponíveis no momento do tratamento", deixa a critério dos responsáveis pelo tratamento quais medidas adotar, a fim de que o processo de anonimização seja eficaz nos termos da lei. Desse modo, uma série de aspectos podem ser levados em consideração, como: quais dados pessoais serão tratados, qual técnica será utilizada, quais parâmetros deverão ser considerados para a técnica e qual política deverá ser respeitada [36]. Assim, vale elucidar que o parágrafo seguinte do Art. 12° — §1° [12] — contribui para determinar o escopo de abrangência desse artigo, isto é, o que é considerado esforço razoável (embasa-se, meramente, em limitação temporal e de custo).

Além disso, nos Art. 7° e Art. 11° [12], é possível evidenciar que tanto para dados pessoais, quanto para dados pessoais sensíveis, a anonimização tem caráter explícito e mandatório quando da realização de estudos por órgão de pesquisa, o que apresenta extrema relevância no contexto acadêmico. A fim de introduzir o conceito de pseudonimização — que será comparado ao apresentado na subseção 2.1.2 — e evidenciá-lo em relação à anonimização, o Art. 13°, que aborda o tratamento dos dados a partir de estudos em saúde pública, elucida no §4° que [12]:

> "Para os efeitos deste artigo, a pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro."

A partir disso pode-se deduzir a principal diferença entre a anonimização e a pseudonimização, isto é, a possibilidade de associação de um indivíduo a partir de dados anonimizados, pela utilização de informação adicional. Assim, a possibilidade de aplicação de um algoritmo em modo invertido — tal como a criptografia — para converter dados anonimizados em dados pessoais apresenta um potencial prático acima do proporcionado pela anonimização. De fato, a anonimização não é aplicável em sua forma prática, visto que exige a exclusão de dados pessoais que possam identificar uma pessoa e tal processo pode inviabilizar o objetivo desejado pelo processamento das informações [37],[34]. A Figura 2.2 ilustra a clara divergência entre as duas técnicas.

Figura 2.2: Diferença entre anonimização e pseudonimização [12].

Além disso, um bom ponto de partida ao se traduzir uma lei para um contexto técnico é identificar os princípios, que são ideais abordados pela lei, de modo abstrato e simples, para introduzir os direitos fundamentais a serem respeitados [38]. Em relação a LGPD, o Art. 6° apresenta dez princípios e, embora não inclua a anonimização em si como um princípio, a mesma pode ser identificada como um subgrupo do princípio da segurança, dado que é impossível alcançar tal ideal sem a desidentificação de dados pessoais sensíveis. Os princípios exaltados pela LGPD são [12]:

1. Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

2. Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

3. Necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

4. Livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

5. Qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

6. Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

7. Segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

8. Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

9. Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

10. Responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Para as leis de privacidade no geral, há uma clara distinção em relação aos dados pessoais de crianças, uma vez que o tratamento dos mesmos é considerado um grande desafio quando há disposição de serviços de terceiros [39]. É necessário que haja garantia por parte da organização de que tais serviços também garantam o tratamento especializado nesse caso. Na lei brasileira, é abordado no Art. 14° [12], que o tratamento deverá ocorrer por meio de consentimento dos pais ou responsável legal, e, vale elucidar que para

quaisquer fins da lei, são consideradas crianças pelo Estatuto da Criança e do Adolescente aquelas que apresentam idade inferior a 13 anos [40].

No que tange os titulares dos dados, há contemplado na LGPD um direito ativo pelo qual os mesmos podem influenciar no tratamento dos dados, inclusive pela atuação como fiscalizadores durante todo o processo [22]. O Art. 18° [12] declara a participação ativa do titular dos dados pessoais na garantia de que seus dados serão tratados adequadamente, pela possibilidade de requerer acesso, anonimização e até mesmo deleção das suas informações. Esse processo se embasa nos princípios de livre acesso e de transparência — explicitados no Art. 6° (IV, VI) [12] —, e proporciona certo arbítrio para fiscalizar os processos de tratamento dos próprios dados, sem desconsiderar o papel da autoridade nacional.

2.1.2 Regulamento Geral sobre a Proteção de Dados

Em toda a União Europeia, há um consenso sobre a lei que regula a proteção de dados pessoais, que é o Regulamento Geral sobre a Proteção de Dados — General Data Protection Regulation (GDPR) —, em vigência desde maio de 2018 [41]. Sendo assim, trata-se de uma legislação precursora à LGPD, ou seja, proporcionou um embasamento em relação ao escopo, aos direitos, aos princípios e à fiscalização para a lei brasileira [42]. Dessa forma, a GDPR igualmente busca resguardar a proteção e a privacidade de dados pessoais de cidadãos europeus, mesmo que o processamento não seja realizado em algum dos Estados-membro [43]. A fim de compreender as principais semelhanças e diferenças, faz-se necessário analisar os principais pontos em que o regulamento é estruturado.

Assim como a LGPD, a GDPR caracteriza dado pessoal — *personal data* — como qualquer informação que identifica ou torna um indivíduo identificável [21]. Além disso, no Art. 9 [41] é elucidado como deve ser o processamento de uma categoria especial de dados pessoais, que são informações que revelam origem racial ou étnica, opinião política, convicção religiosa, etc. – semelhante à definição de dado pessoal sensível na LGPD, explanada na subseção 2.1.1. Um ponto de divergência em relação à LGPD trata-se da inexistência do processo de anonimização na GDPR, sendo exposto apenas a pseudonimização, no Art. 4, que é [41]:

> "[...] o processamento de dados pessoais de tal forma que os dados pessoais não possam mais ser atribuídos a um sujeito de dados específico sem o uso de informações adicionais, desde que tais informações adicionais sejam mantidas separadamente e estejam sujeitas a medidas técnicas e organizacionais para garantir que os dados pessoais não sejam atribuídos a uma pessoa natural identificada ou identificável."

Nesse âmbito, é possível observar que ambas leis conceituam a pseudonimização explicitamente e, embora por si só não seja considerada um princípio, por se tratar de uma

medida de segurança, está intimamente e de modo implícito relacionada ao princípio da Integridade e Confidencialidade, para a GDPR [44], e analogamente ao princípio da Segurança — por meio da relação proposta por Canedo et al. [45] em uma tabela comparativa entre LGPD e GDPR —, para a LGPD. Apesar de não ser considerada um princípio para as leis supracitadas, é inegável sua relevância e indispensabilidade para alcançar a conformidade com tais normas vigentes de privacidade e, de fato, tamanha importância é tida como um princípio em diversas leis, ainda que concomitante com um outro princípio de segurança [23].

Por meio do Art. 4(26) da GDPR [41], os dados anonimizados não são apontados como dados pessoais, semelhantemente à LGPD. Assim, apresentados os tipos de dados e processamento relativo de desidentificação, é relevante exaltar as entidades envolvidas no tratamento dos dados. Ainda no Art. 4, a GDPR estabelece as entidades envolvidas no processo (7–8) e no Art. 39(1), além da entidade fiscalizadora Art. 51 [41]:

4(7). *controller* (controlador): pessoa natural ou jurídica, autoridade pública, agência ou outro organismo que, sozinho ou em conjunto com outros, determina as finalidades e os meios do processamento de dados pessoais;

4(8). *processor* (processador): pessoa natural ou jurídica, autoridade pública, agência ou outro organismo que processa dados pessoais em nome do controlador;

39(1). O *data protection officer* (encarregado de proteção de dados) deve ter pelo menos as seguintes tarefas: (b) monitorar o cumprimento deste Regulamento, bem como de outras disposições de proteção de dados da União ou do Estado-Membro e das políticas do controlador ou processador em relação à proteção de dados pessoais, incluindo a atribuição de responsabilidades, sensibilização e treinamento do pessoal envolvido nas operações de processamento, e as auditorias relacionadas.

51(1). Cada Estado-Membro deve designar uma ou mais autoridades públicas independentes responsáveis por monitorar a aplicação deste Regulamento, a fim de proteger os direitos fundamentais e liberdades das pessoas naturais em relação ao processamento e facilitar o livre fluxo de dados pessoais dentro da União ("autoridade de supervisão").

É possível destacar uma equivalência direta de definição em relação ao controlador e ao operador na LGPD [12], todavia há um papel mais regulatório para o encarregado do que de mediação, que é estabelecido na LGPD. Além disso, a autoridade de supervisão é relativa à cada Estado-membro, o que motiva a descentralização em relação à lei brasileira e a possibilidade de múltiplos agentes regulatórios.

Em relação ao *Data Protection Officer* (DPO), é importante destacar um grande desafio apontado pelas organizações, que é a relação entre os desenvolvedores e o DPO [17]. Isso se deve ao fato de que, uma vez que a GDPR aponta um contexto meramente legal, há uma incompatibilidade da tradução do mesmo para um contexto técnico, dada a complexidade de alinhar as propostas do DPO e as implementações dos desenvolvedores [15]. Dessa forma, é evidente a inclinação em uma atuação regulatória pelo DPO, ao invés de mediadora.

Dito isso, assim como na LGPD, há uma série de princípios na GDPR que contribuem para favorecer uma implementação facilitada e a maior parte deles possuem uma relação direta com princípios da LGPD [45], com exceção de alguns princípios da lei brasileira que são considerados como direitos fundamentais na lei Europeia. No Art. 5 são apresentados sete princípios — em contraste dos dez da LGPD — e não há consideração da anonimização explicitamente como um princípio [25]. Sendo assim, os princípios elucidados no Art. 5 pela GDPR em essência e seus respectivos nomes são [41]:

1. Os dados pessoais devem ser:

   (a) processados de maneira lícita, justa e transparente em relação ao titular dos dados ("licitude, lealdade e transparência");

   (b) coletados para fins específicos, explícitos e legítimos, sem serem processados posteriormente de maneira incompatível com esses propósitos ("limitação de finalidade");

   (c) adequados, relevantes e limitados ao que é necessário em relação aos propósitos para os quais são processados ("minimização de dados");

   (d) precisos e, quando necessário, mantidos atualizados; deve-se tomar todas as medidas razoáveis para garantir que dados pessoais imprecisos, considerando os propósitos para os quais são processados, sejam apagados ou retificados sem demora ("precisão");

   (e) mantidos em uma forma que permita a identificação dos titulares dos dados por não mais do que o necessário para os propósitos para os quais os dados pessoais são processados ("limitação de armazenamento");

   (f) processados de maneira que garanta a segurança adequada dos dados pessoais, incluindo proteção contra processamento não autorizado ou ilegal e contra perda, destruição ou dano acidental, utilizando medidas técnicas ou organizacionais apropriadas ("integridade e confidencialidade").

2. O controlador será responsável por, e capaz de demonstrar conformidade com os princípios acima citados ("responsabilidade").

Uma vez que esses princípios possuem relação direta com os da LGPD e, ademais, com a ISO/IEC 29100–*Information technology–Security techniques–Privacy* framework [18], é importante reforçar a necessidade de compreender os pontos de semelhança e divergência entre as leis de privacidade, dado que princípios equivalentes, logicamente, proporcionarão dificuldades análogas para organizações e desenvolvedores. Sendo assim, o estudo aprofundado dos princípios das leis vigentes é um bom ponto de partida para discutir soluções comuns para desafios das leis vigentes [7].

No que tange os dados pessoais de crianças, há uma clara divergência da lei brasileira, explicitada no Art. 8: considera-se legal a coleta de dados de uma criança, para todo efeito da GDPR, quando ela tiver pelo menos 16 anos [41]. Desse modo, o consentimento pelo responsável legal da criança se faz necessário apenas se a criança tiver menos de 16 anos, e não 13, como consta na LGPD [12]. Sendo assim, a dificuldade quanto à utilização de serviços de terceiros e o tratamento de dados de crianças [16] é ressaltada, uma vez que abrange uma maior parcela da população afetada.

Em relação aos direitos individuais, a GDPR garante uma série de direitos (Capítulo 3 [41]), tais como: o direito de acesso ao processamento dos dados [25]; direito de retificação por parte do titular [46], inclusive em oposição à tomada de decisões automatizadas [25]; e o direito de apagamento ou esquecimento dos dados pessoais, quando atingidas as finalidades [25]. Dessa forma, assim como na LGPD, o titular possui papel ativo no tratamento de seus dados pessoais, sendo necessário apenas conhecer as bases legais.

2.1.3 Lei Americana de Proteção à Privacidade de Dados

Em relação aos Estados Unidos da América (EUA), a embrionária Lei Americana de Proteção à Privacidade de Dados — *American Data Privacy and Protection Act* (ADPPA) — foi apresentada em julho de 2022 como o primeiro projeto de lei abrangente de privacidade de dados dos EUA [21]. Até então, cada unidade federativa teria autonomia para designar frameworks de privacidade a serem seguidos e legislações estaduais, como a renomada Lei de Privacidade do Consumidor da Califórnia – California Consumer Privacy Act (CCPA) [47]. Dessa forma, a ADPPA busca atingir um escopo maior do que a CCPA, isto é, protege dados de pessoais naturais que residem nos EUA, denominados indivíduos [21]. Dito isso, um grande diferencial em relação às leis brasileira e europeia é que ambas leis americanas possuem enfoque maior na liberdade corporativa [48], isto é, há uma maior prospectiva no âmbito de negócios do que nos direitos individuais.

Em relação ao escopo material, a lei define como dado pessoal uma informação que está identifica ou está vinculada, sozinha ou em combinação com outras informações, à indivíduos [21]. Além disso, assim como as outras leis vigentes, a ADPPA apresenta *sensitive covered data* como uma categoria especial de dados pessoais, sendo essa capaz de

apresentar características que poderiam causar discriminação em caso de revelação [21]. Entretanto, o que a diferencia das outras leis é a especificidade dos dados sensíveis citados, que são: identificadores emitidos pelo governo, números de contas financeiras, localização precisa, comunicações privadas e informações relacionadas a indivíduos com menos de 17 anos [21].

No quesito anonimização e pseudonimização, a lei não denomina, nem veicula técnicas para garantir a desidentificação dos dados pessoais, apenas caracteriza na Sec. 2(12) um dado desidentificado. Além de requisitar medidas técnicas razoáveis para re-identificação dos dados pessoais, como as leis brasileira e europeia, a ADPPA estabelece que um dado desidentificado trata-se de [49]:

> "[...] informações que não identificam e não estão ligadas ou razoavelmente ligáveis a um indivíduo distinto ou a um dispositivo, independentemente de as informações estarem agregadas, e se a entidade coberta ou o provedor de serviços".

Embora haja um ponto de semelhança em relação as outras leis, em que dados desidentificados não são considerados para propósitos de dados pessoais, a ADPPA igualmente desconsidera dados de funcionários e dados disponíveis em domínio público como dados pessoais [21]. Desse modo, pode-se reforçar a aplicação da lei americana em um escopo corporativo [48], caso que não se observa com tanta especificidade na LGPD e na GDPR. Dito isso, é relevante elucidar as entidades envolvidas no tratamento dos dados, as quais se diferem das duas entidades principais das leis brasileira e europeia. Nas Sec. 2(9) e Sec. 2(29) são estabelecidos os conceitos de entidade coberta (*covered entity*) e provedor de serviços (*service provider*) [49]. Em suma, têm-se que [49]:

- entidade coberta: qualquer entidade ou qualquer pessoa, que não seja um indivíduo atuando em um contexto não comercial, que, sozinha ou em conjunto com outros, determina os propósitos e meios de coleta, processamento ou transferência de informações cobertas;

- provedor de serviços: uma pessoa ou entidade que coleta, processa ou transfere dados cobertos em nome de e sob a direção de uma entidade coberta ou uma entidade governamental federal, estadual, tribal, territorial ou local. Além disso, recebe dados cobertos de ou em nome de uma entidade coberta ou uma entidade governamental federal, estadual, tribal, territorial ou local.

Isso quer dizer que, a lei é aplicada às entidades cobertas, pessoas ou não, que são responsáveis legalmente pelo tratamento dos dados e aos provedores de serviço, que realizam o tratamento em si. Em relação ao órgão fiscalizador, tem-se na Sec. 2(32) a Autoridade Estadual de Privacidade, que seria o principal oficial de proteção ao consumidor de um

Estado; ou uma agência estadual de proteção ao consumidor com expertise em proteção de dados, incluindo a Agência de Proteção à Privacidade da Califórnia [49]. Além disso, o Procurador Geral igualmente possui deveres regulatórios, inclusive para aplicações de sanções – estabelecidas na Sec. 402 [49].

Embora a lei americana não destaque explicitamente a designação de um encarregado pela proteção de dados, na Sec. 208 há menção da designação de um oficial ou funcionário(s) quando se trata de implementações de medidas de segurança [49]. Dessa forma, é possível exaltar que a presença de um *Data Privacy Officer*, com as mesmas funções da GDPR e da LGPD é meramente parcial na lei americana.

Um significativo ponto de divergência da legislação americana é a descentralização dos princípios adotados pelas outras leis, isto é, não há um capítulo específico que une todos os princípios (e sequer há explicitação de que são princípios). Todavia, é possível observar em algumas seções semelhanças com princípios da GDPR, como pode ser observado a seguir, extraído da lei [49]:

- (Sec. 101) Finalidade: Uma entidade coberta pode coletar, processar ou transferir dados cobertos para qualquer um dos seguintes propósitos, desde que a coleta, processamento ou transferência seja limitada ao que é razoavelmente necessário e proporcional a tal propósito.

- (Sec. 101) Minimização de dados: Uma entidade coberta não pode coletar, processar ou transferir dados cobertos, a menos que a coleta, processamento ou transferência seja limitada ao que é razoavelmente necessário.

- (Sec. 202) Transparência: Cada entidade coberta deve disponibilizar publicamente, de maneira clara, evidente, não enganosa, fácil de ler e prontamente acessível, uma política de privacidade que forneça uma representação detalhada e precisa das atividades de coleta, processamento e transferência de dados da entidade coberta.

- (Sec. 301) Precisão: Um grande detentor de dados deve designar pelo menos 1 dos funcionários descritos no parágrafo (1) para reportar diretamente ao mais alto funcionário do grande detentor de dados como um oficial de proteção de privacidade que deve, além dos requisitos no parágrafo (2), direta ou indiretamente por meio de um designado ou designados supervisionados - (D) Manter registros atualizados, precisos, claros e compreensíveis de todas as práticas materiais de privacidade e segurança de dados empreendidas pelo grande detentor de dados.

- (Sec. 208) Integridade e Confidencialidade: Uma entidade ou provedor de serviços coberto deve estabelecer, implementar e manter práticas e procedimentos razoáveis

de segurança administrativa, técnica e física para proteger e assegurar os dados cobertos contra acesso e aquisição não autorizados.

- (Sec. 301) Responsabilização da corporação: A partir de 1 ano após a data de promulgação desta Lei, um executivo de uma grande entidade de dados deve certificar anualmente, de boa fé, perante a Comissão, de acordo com o método especificado pela Comissão por regulamentação nos termos da seção 553 do título 5 do Código dos Estados Unidos, que a entidade mantém: (1) controles internos razoavelmente elaborados para cumprir esta Lei; e (2) estruturas internas de relatórios para garantir que o executivo certificador esteja envolvido e seja responsável pelas decisões que impactam a conformidade da grande entidade de dados com esta Lei.

A partir disso, pode-se notar correlação entre princípios da GDPR e da LGPD, como os princípios de finalidade e transparência —inclusive dotados de mesmo nome, em múltiplas legislações —, o que pode contribuir na compreensão de leis recentes [20]. Já em relação aos dados de crianças, a entidade coberta precisa, necessariamente, saber que os dados se referem a uma criança, para que não possa compartilhar tais dados (explicitado na Sec. 205) [49]. Todavia, a lei possui uma clara exceção, que contribui para um aspecto mais brando dentre as outras, como exposto na Sec. 205 [49]:

> "A entidade coberta ou provedor de serviços pode coletar, processar ou transferir dados cobertos de um indivíduo que a entidade coberta ou o provedor de serviços sabe que tem menos de 18 anos exclusivamente com o objetivo de fornecer informações relacionadas à vitimização de crianças à aplicação da lei ou à organização sem fins lucrativos, centro nacional de recursos e centro de informações designado pelo Congresso para fornecer assistência a vítimas, famílias, profissionais que atuam em prol das crianças e ao público em geral em questões relacionadas a crianças desaparecidas e exploradas."

Isso quer dizer que, em um aspecto humanitário, é possível realizar o compartilhamento dos dados de crianças, ainda que não se tenha autorização dos responsáveis legais e, caso contrário, o aspecto é proibitivo. Ademais, a lei elucida explicitamente a problemática do compartilhamento de dados de crianças com serviços de terceiros [49].

Já em relação aos direitos legais por parte dos titulares, a legislação estabelece uma série, tais como: a coleta de dados minimizada, em que se visa colher apenas dados extremamente necessários para se atingir a finalidade estabelecida; transferência permitida por dados desidentificados; processamento consistente com propósito (como explicitado no princípio da finalidade); e deleção dos dados ao final do serviço [46].

2.1.4 Lei de Privacidade Australiana

É inegável a massiva quantidade de desafios quando se trata de traduzir leis de privacidade para um contexto técnico, isto é, adequá-las para uma implementação factível nas organizações [18]. Para a lei de privacidade australiana — *Privacy Act 1988* — essa dificuldade é uma ainda mais marcante, uma vez que, por se tratar de uma legislação relativamente antiga, foi marcada por diversas reformulações e emendas [50]. Isso significa que, para se fazer uma análise completa da legislação, é necessário compreender as múltiplas emendas da lei e seus motivos — que quase alcançam uma centena [51] —, não necessariamente centralizadas.

Embora seja necessário uma análise mais complexa, ainda encontra-se algumas semelhanças em relação às leis supracitadas. Em essência, o primeiro objetivo elucidado pela lei é de proteger a privacidade de indivíduos, não sendo especificamente para cidadãos australianos [51]. Dessa forma, a legislação identifica, na seção 6, como sendo dado pessoal uma informação acerca de um indivíduo (pessoa natural) identificado ou razoavelmente identificável [51]. Além disso, um ponto de divergência em destaque, igualmente na seção 6, é que opiniões sobre um indivíduo também são consideradas dados pessoais, sejam verdadeiras ou não e, ademais, estejam registradas em forma material ou não [51]. Assim, é evidente o caráter mais abrangente acerca da privacidade em relação às outras leis.

Do mesmo modo que todas as legislações abordadas, a lei australiana também faz menção às informações sensíveis — vide seção 6 [51] —, que se encontram origem racial ou étnica, opiniões políticas, informações acerca da saúde do indivíduo, etc. Sendo assim, apesar de mais antiga, a lei considera diversos fatores que poderiam causar discriminação em caso de exposição dessas informações. Assim como a lei americana, na seção 7B, não são considerados dados pessoais os de funcionários, para quaisquer parâmetros da lei. Ademais, a legislação sequer faz menção se dados anonimizados são considerados dados pessoais ou não, embora elucide a desidentificação de informações pessoais [51].

Em relação às entidades envolvidas no tratamento dos dados pessoais, tem-se que a lei é aplicável para *APP Entities*, isto é, agências ou organizações submetidas aos princípios australianos de privacidade [51]. Dito isso, a lei não faz menção à classes especializadas de responsáveis, como controladores e processadores presentes na lei europeia, e também não há designação de um DPO para as organizações [51].

Assim como nas leis brasileira e europeia, a legislação australiana é baseada em princípios (treze, no total), denominados *Australian Privacy Principles* (APPs) [50]. Ainda que menos abrangente do que a GDPR em diversos escopos [50], a legislação estipula os seguintes princípios, no Anexo 1 [51]:

1. Gestão aberta e transparente de informações pessoais: garantia de que entidades APP gerenciem informações pessoais de maneira aberta e transparente.

2. Anonimato e pseudonimato: exige que entidades APP ofereçam aos indivíduos a opção de não se identificar ou de usar um pseudônimo.

3. Coleta de informações pessoais solicitadas: define quando uma entidade APP pode coletar informações pessoais solicitadas, sendo que há maiores restrições quanto se trata de informações sensíveis.

4. Tratamento de informações pessoais não solicitadas: descreve como as entidades APP devem lidar com informações pessoais não solicitadas.

5. Notificação da coleta de informações pessoais: define quando e em que circunstâncias uma entidade APP que coleta informações pessoais deve informar um indivíduo sobre certos assuntos.

6. Uso ou divulgação de informações pessoais: descreve as circunstâncias em que uma entidade APP pode usar ou divulgar informações pessoais que detém.

7. Marketing direto: uma organização só pode usar ou divulgar informações pessoais para fins de marketing direto se determinadas condições forem atendidas.

8. Divulgação transfronteiriça de informações pessoais: descreve as medidas que uma entidade APP deve tomar para proteger informações pessoais antes de serem divulgadas no exterior.

9. Adoção, uso ou divulgação de identificadores relacionados ao governo: descreve as circunstâncias em que uma organização pode adotar, usar ou divulgar um identificador relacionado ao governo de um indivíduo como seu próprio identificador.

10. Qualidade das informações pessoais: uma entidade APP deve tomar medidas razoáveis para garantir que as informações pessoais que coleta sejam precisas, atualizadas e completas.

11. Segurança das informações pessoais: uma entidade APP deve tomar medidas razoáveis para proteger as informações pessoais que detém contra uso indevido, interferência, perda e acesso, modificação ou divulgação não autorizados.

12. Acesso às informações pessoais: descreve as obrigações de uma entidade APP quando um indivíduo solicita acesso às informações pessoais que a entidade mantém sobre ele.

13. Correção de informações pessoais: descreve as obrigações de uma entidade APP em relação à correção das informações pessoais que mantém sobre os indivíduos.

Além das semelhanças em alguns princípios com relação às leis de privacidade europeia e brasileira, como de qualidade, segurança e acesso aos dados pessoais, a lei australiana destaca-se em um aspecto: a consideração do anonimato como um princípio [51]. Todavia, quando se trata de um escopo que envolva uma organização e suas funções, isto é, além de informações pessoais, os princípios australianos não cobrem uma gestão de risco tão adequada quanto a GDPR [50]. Dito isso, as organizações seguem um Framework de Política de Segurança Protetiva que, por vezes, complementa a baixa objetividade dos princípios e, ademais, também buscam se adequar às leis avulsas de notificação obrigatória de violação de dados [50]. Nesse ponto, há um claro contraste em relação às outras leis de privacidade, como por exemplo, o enfoque na política de responsabilização em caso de violação de dados na LGPD [12], que não é observada diretamente na lei australiana.

Quando se trata de dados pessoais de crianças, as leis brasileira e europeia possuem um direcionamento quanto ao consentimento (tanto em idade quanto às exceções) e as finalidades [12], [41]. Para a lei australiana, a definição de criança é dada pelo Ato da Família de 1975 [52], que seria um indivíduo com idade inferior a dezoito anos. Logo, não há uma abordagem específica da problemática do consentimento e, ademais, da sua extensão aos serviços de terceiros, para dados de crianças. Por esse âmbito, a lei europeia tem um aspecto mais completo e explícito, que contribui para compreensão de desenvolvedores e até mesmo da própria organização [16].

Por fim, em relação aos direitos legais, a lei australiana garante meios para que o indivíduo possa se resguardar da finalidade em que suas informações pessoais são utilizadas, além de reforçar o direito ao anonimato e a possibilidade de intervir no tratamento dos dados, por meio de acesso, correção e deleção dos mesmos [25]. Todavia, a legislação possui uma menor cobertura quando comparada a GDPR ou a LGPD, visto que não aborda direitos de restrição de processamento, nem de portabilidade dos dados e oposição à tomada de decisões automatizada [25].

2.2 Privacy Framework

Previamente às principais leis de privacidade atualmente formuladas, as orientações — focadas em desenvolvedores — sobre a proteção de dados pessoais eram majoritariamente estabelecidas pelos frameworks de privacidade desde a concepção [23]. A ideia é que, por meio de princípios básicos e explicitados em alto nível (assim como nas legislações), os profissionais envolvidos no projeto e no desenvolvimento de um software possam ter um direcionamento em relação à conscientização de privacidade [23]. Dessa forma, como diversos desses princípios ainda são postos em prática, faz-se necessária a compreensão

desses frameworks, uma vez que podem contribuir para os desenvolvedores na tradução de uma lei para um contexto técnico [13].

Além disso, como abordado na Seção 2.1, as legislações possuem pontos de divergência entre si e, consequentemente, o escopo de atuação pode refletir na escassez de novas diretrizes ou no excesso das mesmas [25]. Sendo assim, ao relacionar princípios e direitos individuais das leis com frameworks populares, pode-se avaliar qual possui um maior nível de abrangência, em se tratando de proteção e privacidade de dados pessoais [53]. Dessa forma, ao invés de optar por seguir exclusivamente diretrizes de um framework específico ou de uma legislação, é mais vantajoso encontrar um meio termo que trata de ambos, de modo a suplementar lacunas de proteção [24]. É nesse âmbito que se encontram dois indispensáveis frameworks: o *Privacy by Design* (PbD) e a ISO/IEC 29100 [23].

2.2.1 Privacy by Design

O PbD apresenta como base a privacidade desde a concepção [34], ou seja, os requisitos de privacidade devem ser tratados pelos desenvolvedores o quanto antes do processo de implementação. Ao longo dos anos, diversos esquemas que implementavam o Privacy by Design foram elaborados, de modo que existam múltiplos princípios e guias de privacidade desde a concepção [53]. Assim, para o atual estudo, a escolha de qual esquema de PbD a ser analisado embasou-se na completude da relação existente entre princípios e direitos individuais das leis com o próprio framework.

O PbD, proposto por Ann Cavoukian em 2009 [54], destaca-se uma vez que todos os princípios de legislações vigentes — mundialmente discutidas — são correlacionados com princípios do próprio PbD [53]. Assim, é fundamentado em sete princípios básicos e, utilizados globalmente, permitem uma certa aplicação facilitada de privacidade e proteção de dados quando se trata de software, principalmente durante o projeto do mesmo [23]. Ademais, é possível notar breve semelhança com alguns princípios ou bases legais das leis tratadas na Seção 2.1, que serão apontados em seguida. Os sete princípios propostos, a descrição dos mesmos e uma breve correlação com os princípios das demais leis (com propósito de contextualização) são [54]:

1. Proativo, não Reativo; Preventivo, não Corretivo

    - Busca-se antecipar e prevenir eventos de invasão de privacidade, isto é, não esperar que uma irregularidade ocorra para contemplá-la. Além de ser integrado à uma boa gestão de riscos, esse princípio apresenta um objetivo principal semelhante ao princípio de Prevenção da LGPD [12].

2. Privacidade por Padrão

- Busca-se garantir a proteção de dados pessoais de maneira automática (*default*), isto é, sem que seja necessário qualquer ação adicional dos indivíduos envolvidos. O princípio possui uma correlação indireta com outros princípios da GDPR, como a limitação de finalidade e a minimização de dados. Além disso, o princípio também é contemplado no Art. 25 da GDPR [41], de modo que fica a cargo do controlador garantir a privacidade por padrão.

3. Privacidade Incorporada ao Design

   - Deve haver integração da privacidade desde a concepção, isto é, até mesmo durante o projeto de um software. Dessa forma, a privacidade deve ser considerada uma funcionalidade por si só, ou seja, indispensável ao funcionamento do sistema. O princípio é igualmente estipulado no Art. 25 da GDPR [41] e, na LGPD, é trivialmente contemplado pelo princípio da Segurança [12].

4. Funcionalidade Completa - Somatório Positivo, não Somatório Zero

   - Busca-se garantir privacidade e outros aspectos simultaneamente, como segurança e desempenho de um sistema, sem que seja necessário realizar um *trade-off* entre os mesmos. Além disso, busca garantir que todos os requisitos estejam otimizados. O princípio dispõe uma ideia de comprometimento, que se relaciona com o princípio de Responsabilização e Prestação de Contas proposto pela LGPD [12].

5. Proteção do Ciclo de Vida de Ponta a Ponta

   - Busca-se garantir a proteção dos dados por todo o ciclo de vida, isto é, desde a coleta até a deleção dos mesmos. O princípio abrange padrões de segurança, tais como confidencialidade, integridade e disponibilidade da informação — assim como os princípios da GDPR [41] —, além de métodos de destruição segura e primitivas criptográficas.

6. Visibilidade e Transparência

   - Busca-se garantir às partes interessadas que os dados são tratados de acordo com a finalidade estipulada e, para comprovação, busca-se a transparência em todas as etapas das operações de tratamento. Dessa forma, está mais relacionado aos princípios de Responsabilização e Prestação de Contas e de Livre acesso, abordados na LGPD [12].

7. Respeito à Privacidade do Usuário

- Busca-se proteger os interesses dos indivíduos em relação à privacidade e, ao mesmo tempo, integrar os usuários como parte ativa no processo de tratamento dos dados pessoais. Os ideais desse princípio encontram-se em múltiplas legislações de privacidade, quando há contemplação de consentimento, acesso e até mesmo revogação dos dados pessoais (os direitos dos indivíduos). Assim, é um princípio que reúne grande parte dos direitos individuais abordados em legislações.

Dessa forma, esses esquemas do PbD são utilizados frequentemente em conjunto com as legislações locais e, ademais, algumas leis incluem explicitamente o PbD em seus artigos, como a GDPR [25]. Isso significa que, em certas legislações, o PbD é legalmente requerido para que se atinja a conformidade e, por conseguinte, a privacidade dos dados pessoais [25]. Por outro lado, em outras diretrizes — como na LGPD — o princípio de Funcionalidade Completa abordado pelo PbD, por exemplo, não é explícito, uma vez que não é apresentado o dilema da privacidade e dos requisitos funcionais [12]. Assim, a utilização do PbD como complemento de legislações pode contribuir para a tradução das mesmas para um contexto técnico.

2.2.2 ISO/IEC 29100

Pouco depois, em 2011, a Força-Tarefa de Tecnologia da Informação ISO/IEC estabeleceu princípios de privacidade e, assim como o PbD, possuem relação direta com princípios e bases legais das legislações da Seção 2.1 [18]. Isso quer dizer que, além de reforçar os parâmetros da lei, o framework pode complementar diretrizes que são abundantes em uma das legislações, mas escassas em outra. Desse modo, a ISO/IEC 29100 — atualizada em 2020 para os padrões brasileiros — trata dos princípios a partir da definição de *Personally Identifiable Information* (PII) [23] ou meramente Dados Pessoais (DP) [55], que seriam informações pessoais capazes de identificar um indivíduo.

Assim, o escopo abordado pelo framework é tão abrangente quanto às legislações, que seria a aplicação para pessoas naturais ou quaisquer organizações envolvidas em tratamento de dados pessoais, que vai desde a especificação até o desenvolvimento e posterior manutenção [55]. Em relação às definições, a norma assemelha-se à LGPD e à GDPR, uma vez que caracteriza dados pessoais sensíveis — que tratam de informações íntimas ao titular —, anonimização e até pseudonomização [55]. Ademais, a ideia do consentimento por parte do titular é semelhante a GDPR (*opt-in*) e os papéis dos envolvidos no tratamento correlacionam-se com os dois principais da LGPD, em adição de um terceiro que pode atuar sob autoridade do operador e do controlador [55].

Com relação ao processo de anonimização, a norma ISO/IEC 29100 estabelece que dados anonimizados não são considerados DP e o processo de pseudonização é semelhante ao discutido na subseção 2.1.1. Isso significa que, tanto para legislações quanto para frameworks, a anonimização de dados pessoais é o começo da garantia de conformidade com as diretrizes. Em seguida, a ISO/IEC 29100 estabelece onze princípios de privacidade — semelhantes aos discutidos na Seção 2.1 —, que são descritos como [23],[55]:

1. Consentimento e escolha: informar os titulares sobre a escolha de permitir ou não o tratamento de DP, seus direitos, informações sobre os processos relativos ao consentimento e, consequentemente, obter o consentimento do titular para coleta e processamento.

2. Especificação e legitimidade de objetivo: garantir que as finalidades estejam em conformidade com a legislação aplicável; comunicar as finalidades aos titulares de DP quando as informações são coletadas ou quando são utilizadas para uma nova finalidade; utilizar linguagem clara e objetiva; explicar, quando convir, o motivo pelo qual serão tratados os DP sensíveis.

3. Limitação de coleta: limitar a coleta de DP aos limites da lei aplicável e estritamente necessária para as finalidades especificadas.

4. Minimização de dados: minimizar a quantidade de DP processada e o número de terceiros envolvidos; tratar apenas os DP necessários para o alcançar os requisitos funcionais; buscar anonimato ou pseudonimização; excluir DP quando a retenção não for mais necessária.

5. Limitação de uso, retenção e divulgação: limitar o uso, retenção e compartilhamento de DP às finalidades especificadas, estabelecidas antes da coleta; manter os DP apenas pelo tempo necessário até que se atinja as finalidades; manter protegidos os DP que requerem retenção.

6. Precisão e qualidade: garantir que os DP tratados sejam precisos, completos e atualizados, bem como confiáveis (quando recolhidos por fontes avulsas ao titular); verificar a validade e correção dos DP antes de fazer quaisquer alterações; garantir a precisão e qualidade desde a coleta até o armazenamento, por meio de verificações periódicas dos DP armazenados.

7. Abertura, transparência e notificação: fornecer informações claras e facilmente acessíveis sobre políticas e procedimentos relativos ao processamento de DP, como a maneira que estão sendo tratados, o objetivo, as partes interessadas envolvidas e a identidade do controlador; divulgar as medidas adotadas pelo controlador que

motivam a limitação do tratamento e do acesso, além de avisar aos titulares sobre quaisquer alterações importantes no tratamento de DP.

8. Acesso e participação individual: fornecer aos titulares de DP a capacidade de acessar e revisar DP, contestar a precisão e integridade, tê-la emendada, corrigida ou removida sem custo ou atraso, sempre garantida de forma simples rápida e eficiente.

9. Responsabilização: documentar e comunicar políticas e procedimentos de privacidade; atribuir indivíduo responsável dentro da organização pela implementação dessas políticas; garantir que terceiros mantenham o nível de privacidade dos DP; fornecer treinamento aos responsáveis pelo tratamento; definir procedimentos de reclamação, informar sobre violações de privacidade, incluindo sanções e compensação.

10. Segurança da informação: proteger DP com controles apropriados nos níveis operacional, funcional e estratégico para garantir a integridade, confidencialidade e disponibilidade de DP ao longo de seu ciclo de vida; escolher operadores de DP que apresentem garantias de conformidade; estabelecer requisitos legais aplicáveis, normas de segurança, análise de riscos e de custo/benefício; priorizar a segurança em DP sensíveis e alto número de DP (que afetaria uma grande quantidade de pessoas em caso de violação); limitar o acesso aos DP apenas ao necessário; solucionar riscos e vulnerabilidades, além de realizar análises periódicas.

11. *Compliance* com a privacidade: demonstrar que o tratamento atende aos requisitos de proteção de dados pessoais; realizar periodicamente auditorias e avaliações de riscos de privacidade; ter controles internos apropriados e mecanismos de supervisão independentes; incorporar análise de riscos em todo processo que envolva tratamento de DP.

Assim, é possível observar que a maioria dos princípios da norma são equivalentes a algum princípio acobertado pela GDPR, embora de escopo menos abrangente do que o PbD [53]. Todavia, com relação aos direitos individuais, a ISO/IEC 29100 aborda meramente os direitos ligados ao consentimento e à reclamação — diretamente ou indiretamente —, como os direitos à informação, de acesso, de retificação e de esquecimento [53].

No que tange o conceito de DP, é interessante elucidar como um indivíduo pode ser identificado meramente pelos seus dados pessoais, mesmo que alguns não sejam tão específicos. Assim, é fundamental distinguir essas informações em dois tipos: identificadores diretos (*identifiers*) e indiretos (*quasi-identifiers*) [56]. Os identificadores diretos são aqueles que, apenas pelo único atributo do dado — como o nome completo ou o Cadastro de Pessoa Física (CPF) — é capaz de identificar um indivíduo. Isso significa que a partir

desse único dado, em caso de vazamento, há possibilidade de associação direta do mesmo com uma pessoa específica. Já os identificadores indiretos carecem de uma combinação de atributos a fim de associar um indivíduo às informações, ou seja, em caso de vazamento de uma parcela desses dados, é incerto afirmar se permite ou não a identificação, sem que se conheça exatamente a combinação dos atributos.

Nos Estados Unidos, a título de exemplo, encontra-se em registros médicos alguns identificadores diretos, como nome e Número de Seguro Social (semelhante ao que é dado como CPF, no Brasil). Além disso, outros identificadores são tidos como indiretos, como idade e tipo sanguíneo [57]. É evidente que a partir de apenas um único identificador indireto, como idade, não é possível identificar um indivíduo com absoluta certeza. A ISO/IEC 29100 estabelece uma série de atributos que podem ser usados para identificar pessoas naturais e, com o intuito de contextualizar os atributos para um escopo nacional, a Tabela 2.1 evidencia determinados identificadores como *identifiers* ou *quasi-identifiers*.

Assim, é inequívoco que os responsáveis pelo tratamento dos dados, se autorizados, poderão identificar dados já anonimizados e associá-los a um indivíduo em específico. Esse processo é denominado re-identificação e, desde que realizado de maneira legítima, isto é, por pessoal autorizado, é juridicamente legal no que tange a LGPD e a GDPR [59]. O grande problema é que, por mais que atributos *identifiers* sejam facilmente definidos e armazenados em centros físicos ou em nuvem, é extremamente complexo definir quais atributos são *quasi-identifiers* [60],[13].

Apesar de parte dos desenvolvedores de software resumirem a dificuldade em traduzir os princípios da lei vigente para a implementação de sistemas [13], o obstáculo é mais abrangente do que parece: é uma solução temporal para uma questão atemporal [56]. Uma vez que a definição de um atributo *quasi-identifier* depende intrinsecamente de outros atributos, é complicado mapear um esquema de dependências. Além disso, a noção de privacidade é mutável, isto é, não é garantido que atributos que antes não transgrediam a privacidade de um indivíduo permaneçam nesse mesmo estado [56]. Por fim, também há dependência em como os atributos são armazenados, uma vez que caso sejam estruturados em documentos não centralizados, a capacidade de identificar atributos relacionados é reduzida, consequentemente.

2.3 Trabalhos Correlatos

Aljeraisy et al. [25] realizaram um estudo comparativo com cinco leis de privacidade, que são de regiões que possuem o inglês como língua primária: a União Europeia, o Canadá, a Califórnia, a Austrália e a Nova Zelândia. Por meio disso, foram identificados princípios chaves e direitos individuais de cada uma das diretrizes e, a fim de que pudessem ser

Tabela 2.1: Identificadores diretos e indiretos no contexto brasileiro [55],[57],[58].

Atributo	**Tipo**
Biometria	*identifier*
Código de Endereçamento Postal (CEP)	*quasi-identifier*
Cadastro de Pessoa Física (CPF)	*identifier*
Data de nascimento	*identifier*
Endereço de e-mail	*identifier*
Endereço IP	*identifier*
Escolaridade	*quasi-identifier*
Gênero	*quasi-identifier*
Nome	*identifier*
Número do cartão de crédito	*identifier*
Número do celular	*identifier*
Profissão	*quasi-identifier*
Registro fotográfico	*identifier*
Renda mensal/anual	*quasi-identifier*
Tipo sanguíneo	*quasi-identifier*
Religião	*quasi-identifier*

comparadas, foi aplicado o método de *Framework Analysis*. Apesar disso, o estudo não inclui a LGPD e é focalizado apenas em princípios e direitos individuais, de modo que não trata de escopo, definições e respectivas sanções.

O estudo realizado por Machado et al. [4] identificou, por meio de um Mapeamento Sistemático da Literatura, os principais desafios que organizações apresentam em se adequar com a GDPR. As dificuldades variam desde problemas relacionados as próprias organizações, tais como disponibilidade orçamentária, falta de time especializado e problemas de desempenho do sistema, até obstáculos relativos a GDPR, como escassez de informações necessárias para implementação, dificuldade em garantir privacidade para serviços de terceiros e manipulação de dados transfronteiriço. Todavia, o trabalho aborda meramente dificuldades relativas à GDPR.

Com o intuito de averiguar o impacto da GDPR em pequenas e médias empresas —

small and medium enterprises (SMEs) —, Li et al. [43] conduziram um estudo etnográfico e identificaram os desafios que se destacam para essas empresas e, não necessariamente, para as de grande porte. Dessa forma, as principais dificuldades encontradas foram: a dependência de testes manuais da GDPR — uma vez que a automatização requer um conhecimento legal abrangente da legislação por parte dos desenvolvedores –; o conhecimento limitado dos requisitos de privacidade (somado a falta de equipe especializada); e o inevitável *trade-off* entre ética e economia, uma vez que é necessário equilibrar a conformidade com a GDPR em um ambiente de negócios competitivo. Dessa forma, todos os desafios apontados são relativos a própria organização, sem tratar àqueles da legislação abordada.

Pensando não apenas em analisar as legislações de privacidade, mas também os frameworks, Barth et al. [23] buscaram unificar as diretrizes disponíveis para desenvolvedores, por meio de codificação de atributos identificados em múltiplas leis e frameworks. Além de investigar os princípios de diversas leis, como a australiana e a europeia, o trabalho aborda os princípios PbD e, semelhantemente, os da ISO/IEC 29100, a fim de identificar semelhanças dos mesmos com as legislações e propor recomendações aos desenvolvedores em situações, por vezes, contraditórias, quando se trata das diretrizes. Todavia, apesar de reunir quatorze diretrizes e codificá-las em uma solução em comum, não há menção à lei brasileira.

O estudo feito por Canedo et al. [45] identificou, por meio de uma revisão sistemática de literatura, diversos modelos e técnicas que os desenvolvedores utilizam para implementar privacidade em software, além de elucidar através de uma pesquisa qualitativa como os profissionais de Tecnologia da Informação e Comunicação entendem a LGPD. O trabalho não só identifica desafios específicos dos desenvolvedores — por exemplo, conhecimento insuficiente e interferência do ambiente organizacional — como também apresenta uma tabela comparativa entre os princípios da LGPD e da GDPR, uma vez que são essencialmente semelhantes aos da ISO/IEC 29100. Assim, os princípios são esclarecidos e alguns direitos individuais são discutidos, porém o aspecto comparativo não é o objetivo principal do trabalho.

Com o objetivo de estabelecer um comparativo aprofundado entre legislações de privacidade, Sangaroonsilp et al. [13] desenvolvem uma taxonomia focalizada em quatro leis e frameworks de privacidade: a GDPR, a ISO/IEC 29100, a Lei de Proteção de Dados Pessoais da Tailândia e o framework da Cooperação Econômica da Ásia e do Pacífico. Para isso, os requisitos das diretrizes são extraídos e refinados, a fim de que possam ser analisados semanticamente e classificados de acordo com suas semelhanças e diferenças. Apesar da GDPR e da ISO/IEC 29100, o estudo é embasado em legislações e frameworks do continente asiático, ou seja, não aborda as leis brasileira, americana e australiana.

Camêlo e Alves [24] implementaram um catálogo de padrão de privacidade, que reúne aspectos da LGPD, do *Privacy by Design* e da ISO/IEC 27701, a fim de facilitar o processo de conformidade com a LGPD para os desenvolvedores. Além de explicitar tarefas relativas ao processamento de dados, como o acesso à informação e a coleta de dados pessoais, um guia é proposto, com o intuito de ajudar os desenvolvedores nos processos de implementação da privacidade em software. Contudo, o estudo é focalizado apenas na legislação brasileira e, quando se trata de manipulação de dados transfronteiriços, deve-se levar em consideração as outras diversas diretrizes envolvidas.

O estudo proposto por Canedo et al. [18] buscou compreender a percepção das equipes ágeis no processo de adaptação a LGPD, isto é, quais mudanças foram necessárias (tanto nos procedimentos, quanto nas equipes) a fim de que a conformidade com a LGPD fosse garantida. Por meio de uma revisão sistemática de literatura, aplicação de survey e triangulação dos de dados, o trabalho identificou diversos desafios apontados pelos profissionais de TI, que variam desde à infraestrutura da organização — como falta de política de segurança e de privacidade de dados — até dificuldades de implementação, como falta de guia ou ferramenta que pudesse auxiliar na elicitação de requisitos de privacidade. Dessa forma, o estudo trata da gradual evolução de conformidade em relação a cada princípio da legislação brasileira.

Ferrão et al. [14] realizaram um estudo que propõe uma taxonomia por meio de um comparativo entre duas legislações (LGPD e GDPR) e um framework (ISO/IEC 29100). A partir de uma Revisão Sistemática de Literatura, o trabalho apresenta descobertas em relação aos requisitos de privacidade propostos pela lei brasileira e pelo framework, isto é, apesar de identificar outras taxonomias presentes na literatura, não foram encontrados previamente estudos que envolvem requisitos da LGPD e do ISO/IEC 29100. Todavia, uma limitação do estudo para dados internacionais seria o escopo tratado, em que os requisitos de privacidade considerados são de duas legislações e um framework.

Diante deste cenário, este trabalho tem como objetivo identificar as principais similaridades e diferenças das legislações abordadas neste capítulo — assim como o exposto por Aljeraisy et al. [25] — e relacioná-las com os frameworks abordados. Além disso, busca identificar e unificar os principais desafios encontrados pelos desenvolvedores em se adequar às legislações [4], [43], [18], por meio da proposição de um guia para apoiar a garantia da conformidade com as leis de privacidade.

2.4 Síntese deste Capítulo

Este capítulo iniciou pela abordagem das legislações vigentes de privacidade de dados, que são utilizadas globalmente, tais como a lei brasileira (LGPD), a europeia (GDPR), a

americana (ADPPA) e a australiana (*Privacy Act*). Foram discutidos os escopos em que as leis são tratadas, definições relevantes, direitos individuais e princípios. Em seguida, os requisitos de privacidade no desenvolvimento de software por meio de frameworks de privacidade, foram apresentados por meio de princípios, focados no Privacy by Design e na ISO/IEC 29100.

Capítulo 3

Revisão Sistemática de Literatura

Para o desenvolvimento dessa pesquisa, foi realizada uma Revisão Sistemática de Literatura (RSL) embasada no trabalho de Kitchenham e Charters [61], em que a metodologia é dividida em três fases:

1. Planejamento: estabelecer a necessidade da revisão sistemática, documentar as etapas necessárias, especificar as perguntas de pesquisa e desenvolver um protocolo de revisão. Os seguintes artefatos encontram-se nessa etapa: perguntas de pesquisa, string de busca e critérios de seleção;

2. Condução da revisão: trata-se dos artefatos da etapa anterior postos em prática, isto é, a execução propriamente dita da revisão e a extração dos dados;

3. Relatório da revisão: é a documentação dos resultados obtidos na revisão, que é formatado por um trabalho acadêmico.

3.1 Questões de Pesquisa

Com o intuito de evidenciar soluções em comum para as múltiplas legislações, a RSL tem o intuito de identificar os desafios apresentados pelas organizações no processo de adequação às leis vigentes dos respectivos países. Ademais, um aspecto facilitador é definir os pontos de convergência e divergência das diretrizes de privacidade. Dito isso, as questões de pesquisa (RQ) que irão direcionar esse estudo são apresentadas na Tabela 3.1.

A RQ.1 tem como meta realizar uma análise comparativa das leis de proteção de dados em quatro regiões distintas, visando identificar tanto as similaridades quanto as disparidades entre elas para compreender as nuances legais e os pontos de convergência entre essas jurisdições, a fim de elaborar uma abordagem abrangente da proteção de dados em um contexto globalizado. É importante ressaltar que a RQ.1 procura extrapolar a

Tabela 3.1: Perguntas de Pesquisa.

ID	Pergunta de Pesquisa
RQ.1	Quais são os principais pontos de semelhança e de diferença entre as leis de proteção de dados do Brasil, da União Europeia, dos EUA e da Austrália?
RQ.2	Quais são os desafios e técnicas apresentados pelas organizações e pelos desenvolvedores ao se adaptarem às leis de proteção de dados no Brasil, na União Europeia, nos EUA e na Austrália?

verificação realizada apenas em princípios e direitos individuais, ou seja, busca identificar comparações entre escopo, definições legais e sanções administrativas das legislações.

A RQ. 2 se concentra-se em investigar os desafios práticos enfrentados por organizações e desenvolvedores ao implementarem e se adaptarem às leis de proteção de dados em diferentes países. A compreensão desses desafios, bem como das estratégias adotadas para lidar com eles, é crucial para elaborar e propor políticas e práticas que promovam a conformidade efetiva e a proteção dos dados em ambientes variados e em constante evolução.

Dessa forma, para responder a RQ.1 será realizada uma RSL que busca identificar, primordialmente, os seguintes dois tópicos: explicação das legislações, isto é, a descrição de pontos específicos para cada jurisdição em questão); e comparação entre as leis, ou seja, informações que destacam semelhanças ou diferenças entre as mesmas, sejam elas explicitamente elucidadas ou não. Semelhantemente, para responder a RQ. 2 será feita uma RSL que pesquisa quatro tópicos: análise de aspectos significativos, que são particularidades relevantes das leis para a conformidade das organizações; desafios comuns, que são aqueles que independem da organização, uma vez que são originados pelas legislações; desafios específicos, que são dificuldades particulares de cada organização; e recomendações práticas, isto é, opiniões de especialistas, das organizações ou de autoridades relevantes.

3.2 String de busca

Para a criação da string de busca, foram estabelecidos quatro pontos essenciais a serem isolados: o nome da legislação (completo ou abreviado), o tipo de comparação, o resultado esperado e a finalidade do estudo. Dessa forma, termos foram identificados para cada um

dos pontos e após múltiplas iterações e respectivos ajustes, a fim de que retornassem a maior quantidade de artigos interessados, a string genérica foi:

> (“LGPD” OR “GDPR” OR “ADPPA” OR “Privacy Act” OR “General Data Protection Law” OR “General Data Protection Regulation” OR “American Data Privacy” OR “Privacy Amendment Act of 2012”) AND (“Comparison” OR “Similarities” OR “Differences”) AND (“Challenges” OR “Opportunities”) AND (“Compliance” OR “Regulation”)

Uma vez que a legislação brasileira poderia ser pouco estudada em artigos escritos em língua inglesa, a string foi adaptada para palavras que correspondem a tradução para o português brasileiro. Assim, ambas foram colocadas em prática e foram obtidos trabalhos escritos tanto em inglês quanto em português. A string genérica utilizada, em português, foi:

> (“LGPD” OR “GDPR” OR “ADPPA” OR “Lei de Privacidade Australiana” OR “Lei Geral de Proteção de Dados” OR “Regulamento Geral sobre a Proteção de Dados” OR “Privacidade de Dados Americana” OR “Lei de Emenda de Privacidade de 2012”) AND (“Comparação” OR “Similaridades” OR “Diferenças”) AND (“Desafios” OR “Oportunidades”) AND (“Conformidade” OR “Regulação”)

Com relação às bases de dados digitais para executar a string de busca, foram escolhidas: ACM Digital Library, IEEE Xplore, Scopus e dblp: computer science bibliography. A razão pela utilização das três primeiras é que são bases já consolidadas em meio acadêmico, além de que indexam relevantes contribuições no meio de engenharia de software e a string de busca genérica necessita de pouca ou nenhuma alteração para dispor resultados interessantes [62]. Ademais, a última também foi escolhida, dado que a base é específica para a bibliografia de ciência da computação, de modo que apresenta resultados recentes e descarta aqueles que não são da área de interesse [63]. A Tabela 3.2 apresenta as strings específicas (adaptadas) utilizadas em cada base, a fim de que retornem mais resultados desejados para o estudo.

Dessa forma, como será mostrado na Seção 3.3, os filtros referentes ao tipo de conteúdo, à data de publicação e à linguagem do artigo foram adicionados manualmente em cada uma das bases, motivo pelo qual não se encontram explicitamente nas strings. Ademais, a busca por termos foi realizada pelo padrão de cada base, isto é, na ACM buscou-se pelo termo identificado em qualquer lugar do artigo, enquanto que no dblp é referenciado apenas pelo título.

Tabela 3.2: Strings específicas para cada base.

Base	String
ACM Digital Library	(“LGPD” OR “GDPR” OR “ADPPA” OR “Privacy Act” OR “General Data Protection Law” OR “General Data Protection Regulation” OR “American Data Privacy” OR “Privacy Amendment Act of 2012”) AND (“Comparison”) AND (“Challenges”) AND (“Compliance”)
IEEE Xplore	(“LGPD” OR “GDPR” OR “ADPPA” OR “Privacy Act” OR “General Data Protection Law” OR “General Data Protection Regulation” OR “American Data Privacy” OR “Privacy Amendment Act of 2012”) AND (“Comparison” OR “Similarities” OR “Differences” OR “Challenges” OR “Opportunities”) AND (“Compliance”)
Scopus	(“LGPD” OR “GDPR” OR “ADPPA” OR “Privacy Act” OR “General Data Protection Law” OR “General Data Protection Regulation” OR “American Data Privacy” OR “Privacy Amendment Act of 2012”) AND (“Comparison” OR “Similarities” OR “Differences”) AND (“Challenges” OR “Opportunities”) AND (“Compliance” OR “Regulation”)
dblp	Privacy Act | LGPD | GDPR | ADPPA Comparison | Similarities | Differences | Challenges | Opportunities | Compliance | Regulation

3.3 Critérios de Seleção

Como técnica de filtragem recomendada dos artigos retornados como resultado da execução da string nas bases de dados digitais [61], foram definidos critérios de inclusão e de exclusão. Os critérios de inclusão demarcam os artigos que se referem ao objeto de estudo deste trabalho, isto é, que são relevantes, compreensíveis e que respondam alguma das perguntas de pesquisa, como apresentado na Tabela 3.3.

Tabela 3.3: Critérios de inclusão.

ID	String
CI1	São aceitos apenas artigos publicados como full papers.
CI2	Os artigos devem abordar especificamente alguma das seguintes leis de proteção de dados vigentes: brasileira, europeia, estadunidense ou australiana.
CI3	Os estudos que destacam os desafios enfrentados pelas organizações ao buscarem conformidade com as leis de proteção de dados no Brasil, União Europeia, EUA ou Austrália.
CI4	Artigos publicados em língua portuguesa ou inglesa.
CI5	Estudos publicados a partir de 2018, isto é, na faixa de 2018–2024.

Dessa forma, é evidente a priorização de estudos que abordam alguma das legislações (CI2) — de maneira unitária ou múltipla, por meio de comparações ou não — e estudos que apresentam as dificuldades que as organizações e, consequentemente, os desenvolve-

dores obtiveram na tentativa de entrar em conformidade com as leis vigentes (CI3). Os critérios CI1 E CI2 de inclusão são focalizados na estruturação do artigo, como descrito anteriormente.

Em relação ao CI5, a escolha da data inicial de publicação é devida a diversos motivos. Tem-se que é o ano em que foi incorporada a lei de privacidade de dados europeia, que representa um marco na proteção de dados em um paradigma digital (e inclusive embasou a legislação brasileira). Além disso, estudos acerca da mesma são encontrados em grande quantidade e é relevante identificar desafios que permaneceram até os dias atuais e, em contrapartida, técnicas que resolveram algumas das dificuldades. Ademais, não é viável selecionar artigos desde 1988 — início da lei australiana, vide subseção 2.1.4 —, uma vez que se busca obter desafios e técnicas atuais.

Os critérios de exclusão, por sua vez, têm o intuito de restringirem ainda mais aqueles artigos selecionados nos critérios de inclusão, isto é, uma segunda filtragem para a priorização de estudos essenciais. Dito isso, os critérios de exclusão são apresentados na Tabela 3.4.

Tabela 3.4: Critérios de exclusão.

ID	**String**
CE1	Estudos que não estão disponíveis em texto completo nas bases digitais utilizadas.
CE2	Estudos que tratam exclusivamente de frameworks, e não das legislações desejadas.
CE3	Estudos que, apesar de abordarem uma das legislações, não apresentam como objeto de estudo a própria legislação.
CE4	Estudos que não apresentam comparações no aspecto legal entre legislações — há abordagem das leis, mas apenas em âmbito explicativo, sem comparações — ou apresentam desafios específicos de um escopo que não seja da engenharia de software.

Como um dos objetivos da RSL é permitir a replicação do estudo em si, conforme indicado por [61], CE1 foi estabelecido a fim de que, inicialmente, apenas artigos facilmente obtidos fossem escolhidos. Trivialmente, uma vez que um mesmo artigo pode ser encontrado em bases digitais diferentes, estudos duplicados foram removidos.

Por fim, com o objetivo de filtrar os artigos às perguntas de pesquisa, segue que: CE2 busca excluir artigos que abordam privacidade em um contexto exclusivo de framework, como apenas Privacy by Design (sem relacioná-lo com alguma lei); CE3 tem o intuito de excluir estudos que não possuem como foco principal uma das legislações, ou seja, aqueles que apenas citam em alguma seção mas não as possui como objeto de estudo; e CE4 busca excluir artigos que tratam de alguma das legislações mas não aplica uma metodologia comparativa, nem identifica desafios relativos às organizações no processo de conformidade com as leis.

3.4 Condução da Revisão

Para a execução da RSL, foi utilizada a ferramenta gratuita Zotero[1], que possibilita a revisão sistemática de literatura através de uma biblioteca de artigos [64]. Uma vez que os estudos foram adicionados, a checagem de duplicados é facilmente realizada, visto que a interface permite uma navegação intuitiva e facilitada, como arquivos de um sistema operacional (de modo que cada arquivo é representado por um estudo). Além disso, os estudos selecionados foram movidos para uma pasta de aceitação e, consequentemente, os demais para a pasta de rejeição. A Figura 3.1 apresenta a etapa inicial de seleção dos estudos.

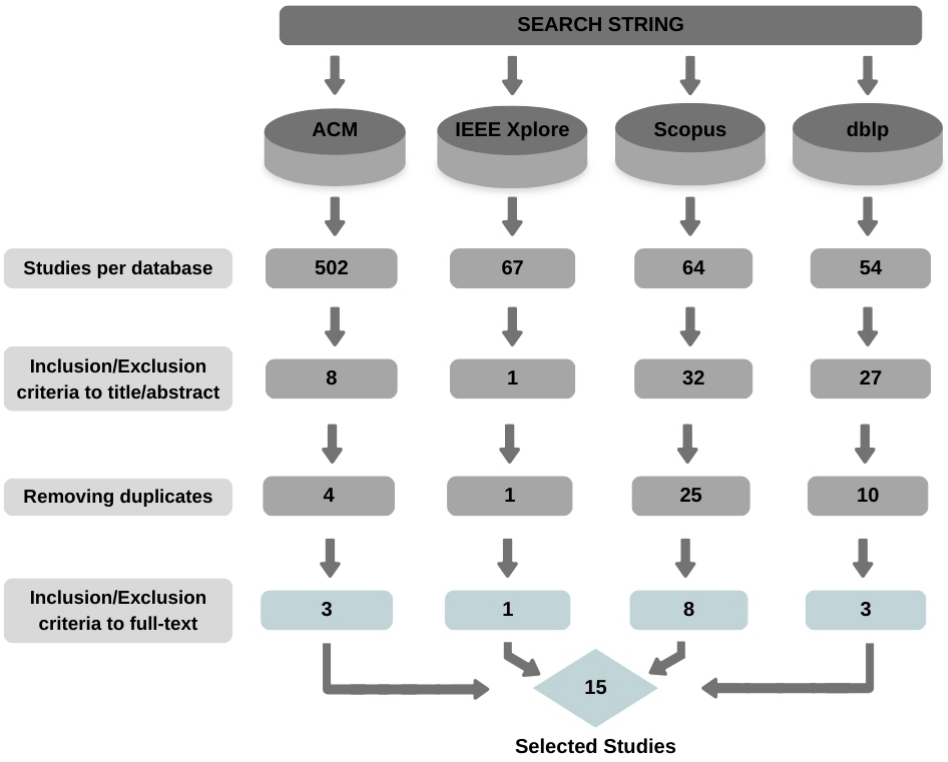


Figura 3.1: Estudos selecionados após cada etapa de seleção.

Assim, por meio da string de busca, foram retornados 687 artigos (502 da ACM, 67 do IEEE, 64 do Scopus e 54 do dblp), como mostrado na Figura 3.1. Após a aplicação dos critérios de inclusão e de exclusão focalizados nos títulos e resumos dos artigos, 648 estudos foram removidos, sobrando 39. A partir da leitura completa desses artigos e, novamente, pela aplicação dos critérios de exclusão, 24 artigos foram removidos e a quantidade final de estudos selecionados foi de 15.

[1] `https://www.zotero.org`

3.4.1 Processo de Snowball

Uma vez que se busca aumentar o número de artigos encontrados para a RSL e mantê-los especializados nas perguntas de pesquisa, foi utilizado o processo de snowball [28], que consiste em iterações de aplicações dos critérios de inclusão e de exclusão para os artigos selecionados até a saturação. Ademais, para cada iteração de snowball, pode-se adotar as técnicas: backward, que extrai novos estudos a partir da leitura das referências de um artigo; forward, que busca estudos que citaram o artigo em questão; ou ambas [65]. Dessa forma, a etapa que extrai os estudos das bases digitais e os seleciona — 15, no caso — é considerada a iteração zero e, para cada artigo, segue a metodologia aplicada [65]:

1. Realização da leitura integral do artigo;
2. Aplicação de snowball backward e forward simultaneamente e escolha de novos artigos;
3. Caso não tenha chegado à saturação, repete-se o processo.

A técnica de snowball backward é trivialmente dada, uma vez que basta a leitura das referências do artigo e aplicação dos critérios de seleção. Para o snowball forward, foi utilizado o Google Scholar, uma vez que a plataforma possui suporte para identificar quais estudos citaram o artigo em análise e, semelhantemente, aplicação dos critérios de seleção para todos os novos estudos identificados.

Para o atual estudo, o processo é mostrado na Figura 3.2 e pode-se observar que a partir dos 15 artigos extraídos inicialmente, foi possível identificar mais 50 potenciais estudos (40 backward e 10 forward) e realizada a seleção de 11 novos. Assim, para cada novo estudo selecionado, uma nova iteração de snowball foi aplicada até que não se encontrasse mais estudos que atendessem aos critérios de inclusão e de exclusão, que é denominado ponto de saturação.

Dessa forma, como observado na Figura 3.2, a saturação ocorreu na sétima iteração, em que foi aplicado o snowball para apenas um único artigo. Sendo assim, para cada iteração, tem-se que a quantidade de novos estudos extraídos é, respectivamente: 11, 11, 8, 5, 2, 1, 0. Isso quer dizer que, pela soma dos 15 estudos iniciais e das iterações, foram selecionados 53 estudos no total (mais do que o triplo estabelecido inicialmente) e foi realizada a leitura integral de cada um. O processo atualizado é representado na íntegra pela Figura 3.3.

O intuito do processo, além de identificar novos materiais de estudo, é delimitar cada vez mais o escopo da pesquisa, ou seja, otimizar a relação entre os artigos que atendem aos critérios de seleção e a seleção propriamente dita. Observa-se, a título de exemplo, que nas

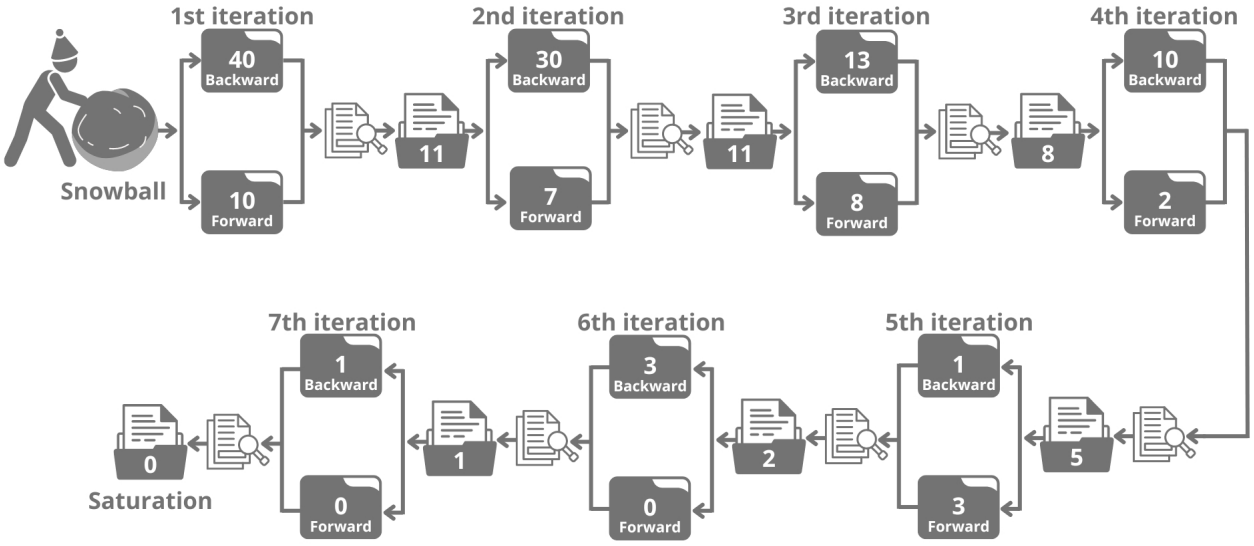


Figura 3.2: Estudos selecionados após cada etapa de snowball.

últimas iterações de snowball cerca de metade dos artigos identificados eram selecionados e extraídos.

3.5 Extração dos Dados

Diante disso, a fim de facilitar a visualização, os 15 estudos iniciais selecionados — denominados de base para o este trabalho — apresentam-se estruturados na Tabela 3.5. Em seguida, na Tabela 3.6 encontram-se os demais estudos que foram selecionados pelo processo de snowball (explicitado na subseção 3.4.1). Em ambas tabelas é possível identificar o ID referente ao estudo, que é utilizado para indexá-lo na subseção 3.6, o título, a referência, o ano de publicação e quais das perguntas de pesquisa é respondida por ele.

Para o processo de extração, foi criada uma planilha com colunas que permitem a identificação do estudo tratado, como por exemplo, ID do estudo, título, autores, nome do periódico/conferência e data de publicação. Além disso, diversas outras colunas com informações relativas aos estudos foram estruturadas, tais como: objetivo do estudo, declarações sobre a(s) lei(s), comparações entre as leis, análise de aspectos significativos (aspectos específicos das leis em cada jurisdição que sejam relevantes para a conformidade das organizações), metodologia utilizada, desafios comuns e específicos às organizações, feedback de especialistas, conclusões do estudo, resultados, recomendações práticas e trabalhos futuros.

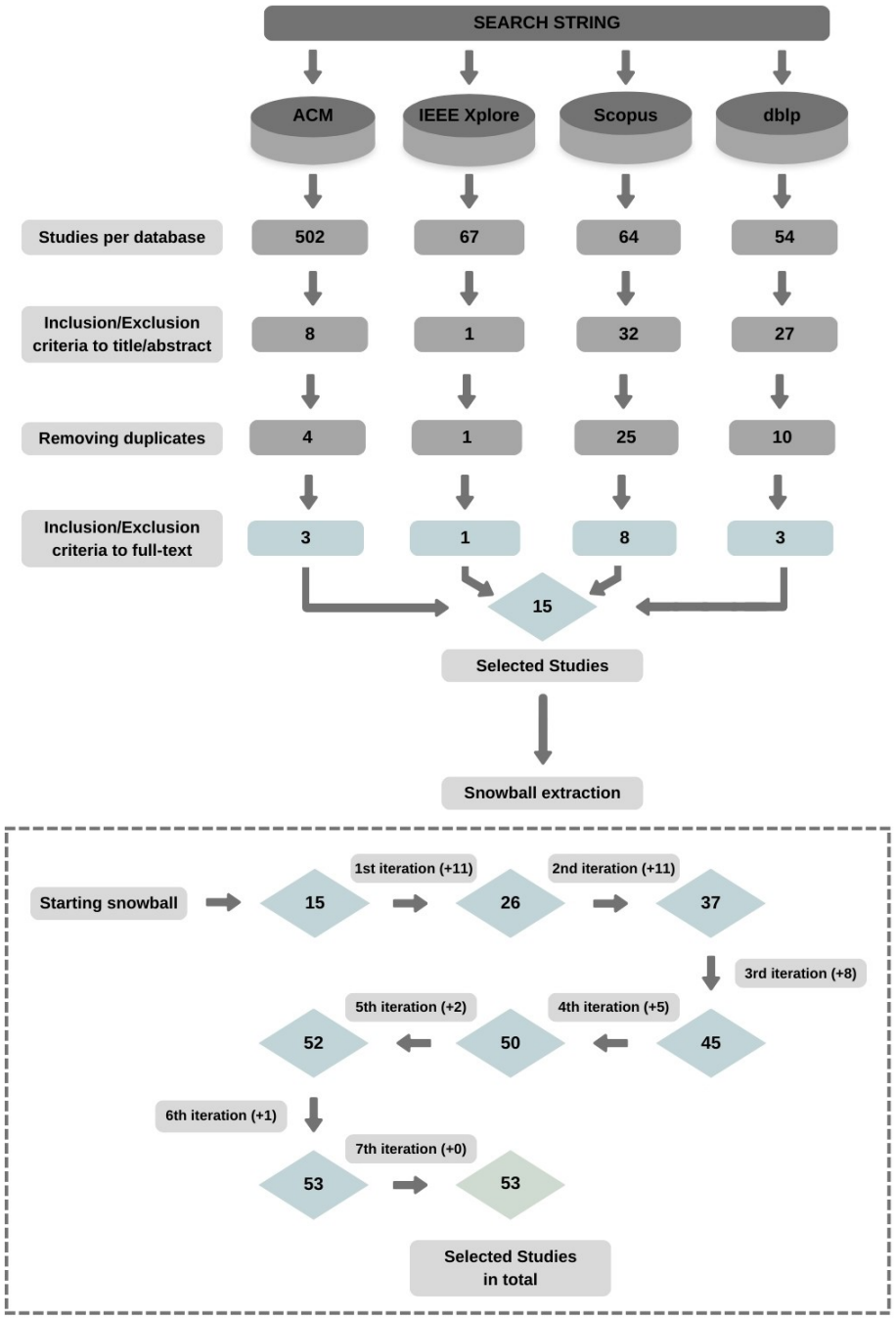


Figura 3.3: Estudos selecionados por meio da RSL e snowball.

Assim, por meio dessa divisão das colunas, é possível identificar facilmente quais estudos atendem a cada uma das perguntas de pesquisa, uma vez que, em caso contrário, haverá uma lacuna na célula da coluna respectiva à informação desejada. Ademais, a coluna de declarações sobre as leis permite uma comparação implícita entre estudos, a fim de otimizar os resultados de RQ.1.

Por fim, a extração dos dados foi realizada por duas pessoas, em que trechos dos

estudos foram individualmente inseridos nas suas respectivas colunas e as mesmas atualizadas quando não os continham. Em caso de discordância, reuniões semanais foram estabelecidas e inclusive motivaram a criação e manutenção de novas categorias. Ao fim da extração, a planilha possuía 53 linhas (uma para cada estudo) e colunas preenchidas para cada informação (e lacunas, em caso de ausência de dados). A lista dos estudos aceitos e as informações extraídas dos estudos encontram-se na plataforma Zenodo [66].

Tabela 3.5: Estudos base selecionados para a RSL.

ID	Título	Ref.	Ano	RQ
E1	A taxonomy for mining and classifying privacy requirements in issue reports	[13]	2023	RQ.1 e RQ.2
E2	The CCPA and the GDPR Are Not the Same: Why You Should Understand Both	[31]	2021	RQ.1
E3	Comparing Data Protection Regulation Models of the EU and the US: Which One Is More Preferred by the Society?	[48]	2022	RQ.1
E4	Análise Comparada entre Regulamentações de Dados Pessoais no Brasil e na União Europeia (LGPD E GDPR) e seus Respectivos Instrumentos de Enforcement	[42]	2021	RQ.1
E5	GDPR e LGPD: estudo comparativo	[38]	2021	RQ.1 e RQ.2
E6	Understanding Philippine National Agency's Commitment on Data Privacy Act of 2012: A Case Study Perspective	[67]	2018	RQ.2
E7	Privacy Legislation as Business Risks: How GDPR and CCPA are Represented in Technology Companies' Investment Risk Disclosures	[68]	2023	RQ.1 e RQ.2
E8	Understanding Ethics, Privacy, and Regulations in Smart Video Surveillance for Public Safety	[46]	2022	RQ.1
E9	Agile Teams' Perception in Privacy Requirements Elicitation: LGPD's compliance in Brazil	[69]	2021	RQ.1 e RQ.2
E10	Guidelines adopted by agile teams in privacy requirements elicitation after the Brazilian general data protection law (LGPD) implementation	[18]	2022	RQ.1 e RQ.2
E11	A systematic study on the impact of GDPR compliance on Organizations	[4]	2023	RQ.2
E12	The GDPR Compliance and Access Control Systems: Challenges and Research Opportunities	[70]	2022	RQ.2
E13	Are We There Yet?: Understanding the Challenges Faced in Complying with the General Data Protection Regulation (GDPR)	[15]	2018	RQ.2
E14	The Proposed American Data Privacy and Protection Act in Comparison with GDPR	[21]	2022	RQ.1
E15	A comparative analysis of personal data protection regulations between the EU and China	[71]	2020	RQ.1

3.6 Resultados da RSL

3.6.1 RQ.1. Quais são os principais pontos de semelhança e de diferença entre as leis de proteção de dados do Brasil, da União Europeia, dos EUA e da Austrália?

Os estudos apresentam os mais diversos pontos de convergência e divergência, que tratam de escopo de abrangência da lei — identificam dados pessoais e as partes envolvidas no

Tabela 3.6: Estudos selecionados a partir de snowball.

ID	Título	Ref.	Ano	RQ	Iteração
E16	"The Grace Period Has Ended": An Approach to Operationalize GDPR Requirements	[72]	2018	RQ.2	1ª Backward
E17	Privacy Laws and Privacy by Design Schemes for the Internet of Things: A Developer's Perspective	[25]	2021	RQ.1 e RQ.2	1ª Backward
E18	The Changing Wind of Data Privacy Law: A Comparative Study of the European Union's General Data Protection Regulation and the 2018 California Consumer Privacy Act	[73]	2019	RQ.1	1ª Backward
E19	Why you should care about GDPR in IoT Enterprises & Solutions	[74]	2021	RQ.2	1ª Backward
E20	It's all fun and games, and some legalese: data protection implications for increasing cyber-skills of employees through games	[75]	2018	RQ.2	1ª Backward
E21	Towards privacy compliance: A design science study in a small organization	[43]	2022	RQ.2	1ª Backward
E22	The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks	[76]	2022	RQ.1	1ª Backward
E23	Using MCDA for selecting criteria of LGPD compliant personal data security	[77]	2020	RQ.2	1ª Backward
E24	I'm all ears! Listening to software developers on putting GDPR principles into software development practice	[78]	2021	RQ.2	1ª Backward
E25	A comparative analysis between General Data Protection Regulations and California Consumer Privacy Act	[47]	2023	RQ.1	1ª Forward
E26	We Are Not There Yet: The Implications of Insufficient Knowledge Management for Organisational Compliance	[17]	2023	RQ.2	1ª Forward
E27	A survey on solutions to support developers in privacy-preserving IoT development	[79]	2022	RQ.2	2ª Backward
E28	Perceptions of ICT Practitioners Regarding Software Privacy	[45]	2020	RQ.1 e RQ.2	2ª Backward
E29	GDPR Compliance in the Context of Continuous Integration	[80]	2020	RQ.2	2ª Backward
E30	Information security frameworks for assisting GDPR compliance in banking industry	[81]	2020	RQ.2	2ª Backward
E31	Toward Data Protection by Design: Assessing the Current State of GDPR Disclosure in Web Applications	[82]	2023	RQ.2	2ª Backward
E32	Challenges Regarding the Compliance with the General Data Protection Law by Brazilian Organizations: A Survey	[83]	2021	RQ.1 e RQ.2	2ª Backward
E33	The benefits and challenges of general data protection regulation for the information technology sector	[84]	2019	RQ.2	2ª Backward
E34	A Framework for GDPR Compliance for Small- and Medium-Sized Enterprises	[85]	2019	RQ.2	2ª Backward
E35	Making Sense of the General Data Protection Regulation - Four Categories of Personal Data Access Challenges	[86]	2019	RQ.2	2ª Backward
E36	Diagnostic of Data Processing by Brazilian Organizations - A Low Compliance Issue	[87]	2021	RQ.2	2ª Forward
E37	"Those things are written by lawyers, and programmers are reading that." Mapping the Communication Gap Between Software Developers and Privacy Experts	[88]	2024	RQ.2	2ª Forward
E38	On Understanding How Developers Perceive and Interpret Privacy Requirements Research Preview	[89]	2020	RQ.2	3ª Backward
E39	Privacy Champions in Software Teams: Understanding Their Motivations, Strategies, and Challenges	[90]	2021	RQ.2	3ª Backward
E40	GDPR Compliance in SMEs: There is much to be done	[91]	2018	RQ.2	3ª Backward
E41	Ensuring Privacy in the Application of the Brazilian General Data Protection Law (LGPD)	[22]	2022	RQ.2	3ª Forward
E42	IoT Security and Privacy Challenges from the Developer Perspective	[92]	2023	RQ.2	3ª Forward
E43	Privacy Compliance in Software Development: A Guide to Implementing the LGPD Principles	[7]	2023	RQ.1 e RQ.2	3ª Forward
E44	Data Protection Officers' Perspectives on Privacy Challenges in Digital Ecosystems	[93]	2022	RQ.2	3ª Forward
E45	"It may be a pain in the backside but..." Insights into the resilience of business after GDPR	[94]	2022	RQ.2	3ª Forward
E46	The Critical Success Factors of GDPR Implementation: A Systematic Literature Review	[95]	2019	RQ.2	4ª Backward
E47	A review of information privacy laws and standards for secure digital ecosystems	[50]	2018	RQ.1 e RQ.2	4ª Backward
E48	The General Data Protection Regulation in Financial Services Industries: How Do Companies Approach the Implementation of the GDPR and What Can We Learn From Their Approaches?	[96]	2020	RQ.2	4ª Backward
E49	A Narrative Review of Factors Affecting the Implementation of Privacy and Security Practices in Software Development	[60]	2023	RQ.2	4ª Forward
E50	Developers Say the Darnedest Things: Privacy Compliance Processes Followed by Developers of Child-Directed Apps	[39]	2022	RQ.1 e RQ.2	4ª Forward
E51	A Review of GDPR Impacts on Information Security	[97]	2022	RQ.2	5ª Forward
E52	Navigating the Data Avalanche: Towards Supporting Developers in Developing Privacy-Friendly Children's Apps	[16]	2023	RQ.2	5ª Forward
E53	"Money makes the world go around": Identifying Barriers to Better Privacy in Children's Apps From Developers' Perspectives	[98]	2021	RQ.2	6ª Backward

tratamento —, de definições legais específicas de cada lei, de direitos individuais, de princípios e, como consequência de não conformidade, as sanções administrativas. Os estudos relacionados ao regimento europeu — General Data Protection Regulation (GDPR) — são facilmente encontrados, inclusive em comparações com a própria Lei Geral de Proteção de Dados (LGPD). O maior entrave foi em identificar estudos que relacionassem a legislação americana — American Data Privacy and Protection Act (ADPPA) — com as demais, visto que é a mais recente dentre os objetos de estudo deste trabalho. Para suprir essa necessidade, resultados acerca da lei de privacidade da Califórnia — California Consumer Privacy Act (CCPA) — também foram extraídos, dada a certa semelhança legal e regional.

Com relação ao escopo de abrangência, um fator de semelhança entre a LGPD e a GDPR é o consentimento orientado pelo *opt-in* (E9[69], E10[18]), isto é, os titulares dos dados explicitam que aceitam o tratamento antes do seu início (por meio de políticas que envolvem termos de uso ou *cookies*). Não só isso, mas também o consentimento em si é considerado como um direito individual de ambas leis. Dito isso, um tópico de divergência em relação às leis brasileira e europeia, é o consentimento no estilo *opt-out* realizado pela CCPA (E2[31], E18[73]).

A garantia, por lei, de que os dados pessoais de indivíduos serão protegidos é unânime, embora as legislações norte-americana e canadense apresentem um enfoque orientado à empresas e funcionários (E1[13], E14[21], E25[47]), o que apontam para uma maior priorização da liberdade corporativa do que nos direitos de privacidade de um indivíduo (E3[48]). Assim, um importante ponto de divergência relativo à essa área é que dados pessoais de funcionários, por exemplo, são alheios à aplicação da ADPPA, enquanto são contemplados pela GDPR (E14[21]).

Quando se trata de escopo territorial, a LGPD e a GDPR apresentam atuações semelhantes, em que mesmo que as organizações não estejam fisicamente localizadas no Brasil ou na União Europeia, respectivamente, ainda assim a legislação pode vir a ser aplicável, sendo necessário apenas que ofereçam serviços ou processem dados dos cidadãos (E10[18], E21[43]). Dessa forma, apesar de ser necessário um maior grau de fiscalização, a GDPR apresenta entre as leis a maior autonomia para suas agências reguladoras, devido a maturidade legal e arcabouço teórico disponível, inclusive quando comparada à outras leis (E4[42], E15[71]).

No que se refere os dados pessoais sensíveis, todas as legislações apresentam uma categoria especial que os define (E14[21], E32[83], E43[7], E47[50]), o que é um marco de semelhança, e as definições dos mesmos são parecidas, como origem racial ou étnica, opinião política e dado referente à saúde. Todavia, a especificação dos dados sensíveis apresentada pela ADPPA é mais explicativa do que a GDPR (E14[21]), e consequente-

mente, do que a LGPD. Além disso, informações que contribuem para a identificação de um indivíduo (não diretamente) são considerados dados sensíveis na GDPR, enquanto a associação é meramente direta na LGPD (E32[83]). Vale lembrar que, como explicitado na Seção 2.1, um ponto diferencial da lei australiana é que a mesma considera uma opinião sobre um indivíduo como um dado pessoal.

A maioria das leis — LGPD, GDPR, ADPPA e CCPA — especificam entidades responsáveis pelo tratamento dos dados pessoais (E1[13], E8[46], E12[70], E14[21], E41[22]) e, ademais, as identificam por classes como operador, controlador, encarregado — *Data Protection Officer* (DPO) na GDPR (E26[17], E33[84]) —, processador, etc.

Já no âmbito das definições, um ponto de divergência aflora ao identificar que os indivíduos que são respaldados pelas legislações apontam um caráter mais inclusivo da GDPR do que da CCPA e do que da ADPPA (E7[68], E14[21], E22[76], E25[47]), visto que nessa última estão incluídos apenas cidadãos residentes dos Estados Unidos, enquanto que na CCPA considera-se apenas dados envolvidos em transações financeiras. Não só isso, mas a lei de privacidade australiana apresenta a menor área de cobertura, quando comparada com a GDPR (E47[50]), a ponto de reforçar a ideia de que a GDPR tenha um escopo mais completo na garantia da privacidade. Um outro ponto de divergência é quanto ao consentimento de crianças para o tratamento dos dados: na GDPR crianças não podem consentir e, já na CCPA, o consentimento é livre a partir de 13 anos (E50[39]).

Em relação ao ciclo de vida do dado pessoal, existem algumas notáveis semelhanças e diferenças entre a GDPR, a CCPA e a ADPPA (E8[46]): a coleta é minimizada nas leis europeia e norte-americana, mas é mais flexível na legislação da Califórnia (basta notificar os titulares); a transferência é diferente nas três leis, uma vez que é orientada à contestação do usuário na GDPR, permitida por dados desidentificados na ADPPA e permitida meramente por aviso prévio na CCPA; o processamento é semelhante na GDPR e na ADPPA, apenas consistente com os propósitos, enquanto na CCPA é requerida apenas pseudonimização; e a retenção diverge-se, de tal modo que é consistente com as finalidades na GDPR, via de regra ao final do serviço ou quando solicitada por lei na ADPPA e embasada no pedido do usuário na CCPA (apesar de apresentar direito à exclusão evidenciado (E18[73])), o que evidencia novamente o processo de *opt-out*.

Além da LGPD e da GDPR apresentarem uma série de direitos individuais e princípios equivalentes (E9[69], E10[18]), uma parte dessas bases se alterna, isto é, os princípios de livre acesso, prevenção e não discriminação estabelecidos pela LGPD não possuem equivalência direta com algum princípio da GDPR, uma vez que são abarcados pelos direitos individuais na legislação europeia (E28[45]). Igualmente, a legislação australiana estabelece direitos semelhantes a GDPR (E17[25]), todavia não apresenta direitos de restrição de processamento, portabilidade dos dados e nem de oposição à tomada de

decisões automatizada.

Quanto aos comparativos entre os princípios, a LGPD apresenta dez princípios fundamentais e a GDPR sete (E10[18]) e, embora sejam parecidos entre si, alguns trabalhos ainda discordam acerca da equivalência entre os mesmos: há elucidação que os princípios da GDPR da licitude, lealdade e transparência, além da limitação de armazenamento, não possuem equivalência direta com qualquer outro princípio da LGPD (E5[38]), enquanto que há uma tabela comparativa que os relaciona aos princípios de transparência e da necessidade (E28[45]). Assim, a se depender da referência, esses pontos podem ser considerados de semelhança ou de diferença. Um importante aspecto de divergência é que na GDPR a anonimização não é considerada explicitamente um princípio — semelhantemente na LGPD —, mas na legislação australiana sim (E17[25]).

Por fim, é identificado nos estudos um ponto de divergência quanto às sanções administrativas aplicadas pela GDPR das aplicadas pela CCPA, que em regra tem-se que na lei europeia as infrações podem impor multas de até 20 milhões de euros ou 4% do volume de negócios global de uma organização (E7[68], E16[72], E21[43], E25[47]). Na CCPA, por sua vez, as multas por não conformidade são referentes à cada violação (até 7500 dólares por violação, sem que haja limite para um número de violações) (E7[68]) e danos estatutários variam de 100 a 750 dólares (E25[47]). Assim, a depender da quantidade de violações, as sanções aplicadas pela CCPA podem superar os valores registrados na GDPR. E na LGPD, é comum a aplicação de multas simples, que alcançam até 2% do faturamento, limitada à 50 milhões de reais (E4[42])

Assim, a Tabela 3.7 elucida os principais pontos de semelhança e diferença abordados nos estudos. O processo de framework analysis a ser adotado objetiva preencher as lacunas faltantes, com o intuito de realizar uma comparação efetiva entre as legislações e associá-las aos frameworks. Além disso, foi realizada uma revisão detalhada dos temas abordados por uma pesquisadora pós-doutora em Ciência da Computação da Universidade Federal de Pernambuco (UFPE), com foco em Direito Digital e Proteção de Dados, que contribuiu para a validação dos temas escolhidos, verificando se eram adequados e faziam sentido no contexto das legislações.

RQ.1 Summary: A GDPR é a lei que possui maior abrangência e cobertura à proteção de dados pessoais dentre as legislações analisadas — seguida pela LGPD —, uma vez que apresenta elevado nível de maturidade legal em relação às outras. Apesar de a ADPPA ser a mais recente, o enfoque econômico por vezes sobrepõe o direito de privacidade (assim como a CCPA) e a lei australiana (a mais antiga), por sua vez, possui um escopo pouco abrangente quando comparada à leis atuais.

Tabela 3.7: Comparações entre as legislações.

Tema	LGPD	GDPR	ADPPA	Privacy Act	CCPA
Escopo Pessoal	Consentimento *opt-in*; Enfoque na proteção de dados	Consentimento *opt-in*; Enfoque na proteção de dados (grande abrangência); Crianças não podem consentir	Consentimento *opt-out*; Enfoque na liberdade corporativa	Consentimento *opt-in*; Enfoque na proteção de dados (menor abrangência); Não diferencia os responsáveis pelo tratamento	Consentimento *opt-out*; Enfoque na liberdade corporativa; Crianças podem consentir a partir de 13 anos
Escopo Territorial	Aplica-se a organizações no Brasil ou fora, desde que trate dados brasileiros	Aplica-se a organizações na U.E ou fora, desde que trate dados europeus	Aplica-se apenas ao processamento de dados de indivíduos residentes dos Estados Unidos	Aplica-se às entidades APP (organizações) que podem ou não estar na Austrália	É aplicada a qualquer entidade com fins lucrativos que faz negócios na Califórnia
Escopo Material	Dado pessoal sensível (associação direta)	Dado pessoal sensível (associação direta e indireta); Compreende dados pessoais de funcionários	Dado pessoal sensível; Não compreende dados pessoais de funcionários	Dado pessoal sensível; Compreende opinião como dado pessoal	Dado pessoal sensível; Não compreende dados pessoais de funcionários
Definições	Define responsáveis pelo tratamento (controlador, operador e encarregado)	Define responsáveis pelo tratamento (controlador, processador e DPO)	Define responsáveis pelo tratamento (entidades cobertas e provedores de serviço)	Define entidades APP	Define negócios e provedores de serviços
Direitos	Consentimento e Escolha; Confirmação da existência dos dados; Acesso aos dados; Correção de dados; Anonimização; Eliminação de dados desnecessários; Acesso à informação das entidades participantes; Portabilidade dos dados; Revogação do consentimento	Consentimento e Escolha; Coleta minimizada; Transferência orientada à contestação; Processamento consistente com as finalidades; Retenção consistente com as finalidades; Direitos de restrição de processamento, portabilidade dos dados e oposição à tomada de decisões automatizadas	Coleta minimizada; Transferência orientada à dados desidentificados; Processamento consistente com as finalidades; Retenção ao final do serviço ou solicitada por lei	Sem direitos de restrição de processamento, portabilidade dos dados e oposição à tomada de decisões automatizadas	Coleta flexível; Transferência orientada à aviso prévio; Processamento livre desde que haja pseudonimização; Retenção embasada no pedido do usuário
Princípios	10 princípios fundamentais; Discute-se equivalência com princípios de licitude, lealdade e transparência e limitação de armazenamento; Anonimização não é um princípio	7 princípios fundamentais; Sem equivalência com princípios de livre acesso, prevenção e não discriminação; Anonimização não é um princípio	-	13 princípios fundamentais; Anonimização é um princípio	-
Sanções	2% do faturamento (limitado à 50 milhões de reais) ou multa diária	20 milhões de euros ou 4% do volume de negócios global	Sem multas administrativas especificamente definidas, mas organizações que infrinjam o ADPPA ainda podem estar sujeitas a ações de aplicação governamentais e direitos de ação privados	-	7500 dólares por violação e danos estatutários entre 100 e 750 dólares

3.6.2 RQ.2. Quais são os desafios e técnicas apresentados pelas organizações e pelos desenvolvedores ao se adaptarem às leis de proteção de dados no Brasil, na União Europeia, nos EUA e na Austrália?

Inicialmente, foram identificados diversos desafios que variam desde o domínio das organizações até os desenvolvedores, a fim de se alcançar a conformidade com as múltiplas legislações. Canedo et al. (E10[18]) e Machado et al. (E11[4]), elucidam a maioria das classes de desafios a serem evidenciadas, referentes à LGPD e a GDPR, respectivamente. A partir de todos os estudos selecionados, foram identificados 168 desafios isolados e, uma vez categorizados em classes embasadas na semelhança desses desafios, foram obtidas 18 classes, conforme apresentado na Tabela 3.8, ordenadas por quantidade. A discussão dos desafios e das respectivas técnicas adotadas para mitigação dos mesmos são discutidas a seguir:

D1) Escassez de conhecimento da lei: Foi o principal desafio identificado na RSL, de modo que abrange duas situações: a falta de conscientização acerca da necessidade de se implementar privacidade em software (E13[15], E17[25], E16[72]); e o baixo ou

Tabela 3.8: Desafios apresentados pelas organizações e pelos desenvolvedores no processo de conformidade com as legislações de privacidade.

ID	Desafio	Referência	Qtd.
D1	Escassez de conhecimento da lei	[18],[13],[67],[15],[72],[25],[74],[43],[78],[17],[45],[80],[85],[7],[94],[89],[90],[91],[95],[39],[69]	21
D2	Traduzir lei para contexto técnico	[18],[4],[13],[13],[15],[72],[78],[17],[79],[86],[94],[90],[16],[69],[22],[92]	16
D3	Restrições de orçamento	[18],[4],[67],[72],[74],[78],[80],[84],[86],[7],[94],[95],[68],[82]	14
D4	Falta equipe com expertise	[4],[74],[43],[80],[84],[87],[79],[7],[94],[91],[95],[60],[82],[83]	14
D5	Estrutura organizacional	[18],[67],[43],[17],[80],[87],[86],[88],[7],[93],[90],[91],[69],[22]	14
D6	Ambiguidade da lei	[4],[70],[15],[72],[25],[43],[80],[93],[94],[60],[95],[96],[97]	13
D7	Falta padronização de técnicas/ferramentas	[18],[17],[80],[86],[7],[89],[90],[95],[97],[98],[83]	11
D8	Falta política de segurança/privacidade	[18],[80],[86],[91],[39],[16],[75],[77],[82],[83]	10
D9	Relacionamento com o usuário	[80],[84],[86],[7],[93],[90],[68],[69],[75]	9
D10	Priorização de requisitos funcionais	[4],[78],[43],[80],[84],[7],[94],[90]	8
D11	Incerteza dos processos organizacionais	[4],[84],[81],[86],[93],[60],[77],[22]	8
D12	Dificuldades em serviços de terceiros	[4],[84],[86],[91],[39],[16],[68]	7
D13	Escassez de guias/ferramentas	[18],[13],[78],[7],[98]	5
D14	Processamento de dados internacionais	[4],[13],[15],[93][68]	5
D15	Mudanças nos estágios de desenvolvimento	[18],[43],[80],[84]	4
D16	*Trade-off* ética x economia	[38],[67],[80],[68]	4
D17	Identificação de requisitos de privacidade	[18],[13],[89],[69]	4
D18	Impacto na usabilidade da aplicação	[85]	1

nenhum conhecimento à respeito da legislação, isto é, a escassez de conhecimento teórico em relação a lei vigente (E10[18], E43[7], [78]). Peixoto et al. (E38[89]) relataram que, por mais que os desenvolvedores possuam conhecimento empírico sobre privacidade, o grande entrave é saber interpretar os requisitos de privacidade, uma vez que grande parte deles não possuem conhecimento formal acerca da privacidade e da LGPD. Assim, as práticas que as organizações têm adotado em busca de solucionar esse desafio é através do treinamento e mentoria para os desenvolvedores (E39[90]), inclusive é sugerido a aplicação de seminários (E13[15]).

D2) Traduzir lei para contexto técnico: Um grande problema apontado por desenvolvedores de diferentes regiões (submetidos à diversas leis de privacidade) é a leitura de normas expressamente teóricas, em que não há especificação de técnicas para se atingir a conformidade (E45[94], E39[90], E26[17]). Dessa forma, como a aplicação de métodos depende de conhecimento prévio do desenvolvedor (E39[90], E24[78]), a tradução de requisitos da legislação para o contexto de privacidade dentro de um escopo específico da organização é de profunda complexidade técnica e grande parte dos desenvolvedores não se sentem confortáveis nesse quesito (E39[90]). Não só isso, mas desenvolvedores também apresentam entraves quando se trata de processos que envolvam anonimização e automação dos dados (E35[86]). Para suprir a falta de especificação de técnicas nas leis, a adoção de frameworks mais específicos é uma solução em comum aos desenvolvedores (E11[4]), uma vez que permite a combinação das normas da legislação vigente com o framework escolhido (E27[79]). Ademais, Kuhtreiber et al. (E27[79]) adicionaram que a utilização de

ferramentas que analisam fluxo de dados e identificam dados sensíveis — como FlowFence, SainT e Databox — contribuem nesse aspecto.

D3) Restrições de orçamento: Trata-se de um entrave comum que engloba apenas as organizações, isto é, os desenvolvedores tem pouca ou nenhuma influência acerca do mesmo (E46[95], E29[80]). Cerca de um ano após a GDPR entrar em vigor, Teixeira et al. (E46[95]) evidenciaram em seu estudo que o processo de conformidade com a lei é custoso e demorado, dado que necessita de recursos financeiros e humanos recorrentes, embora as organizações os tenha de modo limitado (E29[80], E43[7]). Poritskiy et al. (E33[84]) ainda associaram as operações de segurança com o aumento de orçamento das organizações, ou seja, o nível de privacidade e segurança dos dados pode estar intimamente ligado ao capital disponível para garantia dos mesmos. Para pequenas e médias empresas, esse desafio é ainda mais crítico (E40[91]) e uma solução proposta por Brodin et al. (E34[85]) seria a utilização de um design proativo de privacidade, que revela o contraste com a solução elaborada por Ayala-Rivera (E16[72]), em que requisitos de solução vinculam as normas da GDPR e os requisitos comerciais.

D4) Falta equipe com expertise: Difere-se do desafio de escassez de conhecimento da legislação pela seguinte motivação: nesse contexto, as empresas necessitam de pessoal administrativo adicional (E45[94]) e, ademais, pessoal especializado em DPO (encarregado pela proteção de dados) (E36[87], E46[95]). Dito isso, a falta de uma equipe com expertise na legislação vigente pode ocasionar uma avaliação de risco ineficaz na proteção de dados [74] e, acerca da legislação brasileira, as orientações do Guia de Boas Práticas da LGPD podem não ser respeitadas em completude (E36[87]). Uma relevante solução, como supracitado, é a designação de um DPO dentro da própria organização (E36[87], E46[95]) e, no caso da GDPR, a adoção de um controlador permite até restringir o fluxo de dados no sistema (E27[79]).

D5) Estrutura organizacional: Horstmann et al. (E37[88]) apontaram que, muitas vezes, os especialistas em privacidade de uma empresa não compreendem os desenvolvedores de software, e vice-versa. Isso significa que, por meio desse entrave na comunicação (estabelecido na estrutura da organização), os desenvolvedores podem não vir a implementar a privacidade adequada nas aplicações, uma vez que não possuem os respectivos códigos de conduta. Além disso, não é incomum que a própria organização estabeleça limitações aos seus funcionários (E43[7], E10[18]), de modo que a conformidade regulatória não seja alcançada, devido à escassez de comunicação entre as equipes da organização (E26[17]). Sendo assim, Davier et al. (E26[17]) afirmaram que a gestão do conhecimento, dentro de uma empresa, é a chave para uma organização interna eficaz e um processamento de informações em conformidade com as legislações. Além disso, projetos de comunicação como um plano estratégico de sistemas de informação (E6[67]) ou o Programa Instituci-

onal de Privacidade de Dados (E36[87]) podem adequar as organizações e aperfeiçoar a cultura praticada.

D6) Ambiguidade da lei: Aljeraisy et al. (E17[25]) elucidaram que grande parte dos desenvolvedores certamente apresentarão dificuldades em cumprir regulamentos quando estes são vagos, uma vez que dificulta o processo de extração e implementação desses requisitos legais. Não só isso, mas também uma vez que os requisitos não são abordados em linguagem simples e específica, os mesmos ficam abertos à múltiplas interpretações (E12[70], E29[80]), o que pode garantir certo nível de privacidade, mas nem sempre o desejado pela legislação. Aljeraisy et al. (E17[25]) também propõe soluções para o problema da ambiguidade das legislações, como um mapeamento entre a lei de privacidade e esquemas de privacidade desde a concepção (contemplados na Seção 2.2), além da utilização de padrões de projeto como a criptografia por meio de uma chave gerenciada pelo usuário, a ofuscação de medição com adição de ruído (para evitar vazamento de dados sensíveis) e um padrão de notificação de violação de dados.

D7) Falta padronização de técnicas/ferramentas: O estudo proposto por Tahaei et al. (E39[90]) evidenciou que há carência de padronização e métricas de avaliação, uma vez que a conceituação de privacidade é volátil, isto é, apesar de existirem taxonomias e frameworks que conceituam como a privacidade deve ser implementada, não há um consenso entre todas. Para ressaltar esse ponto, os estudos mostram que a decisão sobre a privacidade depende de cada projeto (E38[89]) e as legislações disponíveis não fornecem diretrizes específicas acerca das tecnologias a serem utilizadas, ou seja, as organizações devem encontrar as soluções específicas para si (E46[95]). Em suma, tem-se que não há uma padronização de técnicas, ferramentas ou metodologias adotada para que se atinja a conformidade com as legislações, e é um desafio estabelecer diretrizes de design adequadas e específicas (E10[18], E26[17], E43[7], E51[97], E53[98]). Os estudos evidenciaram possíveis soluções, tal como orientar-se pelas diretrizes da plataforma de publicação da aplicação (E53[98]).

D8) Falta política de segurança/privacidade: A elaboração de um termo de consentimento e, ademais, de uma política de segurança trata-se de um desafio que ainda hoje é negligenciado por parte das organizações (E10[18], E29[80], E35[86]). O trabalho de Freitas et al. (E40[91]) apontou que a maioria das empresas envolvidas não possuíam um registro de medidas de segurança e, além disso, nenhuma empresa apresentava um procedimento que notificava à autoridade em caso de violação dos dados pessoais. Além da negligência das organizações, o desafio pode ter origem do próprio desenvolvedor, uma vez que quando utilizam bibliotecas de terceiros, o mesmo não possui uma compreensão completa das suas aplicações e inviabiliza a elaboração adequada de uma política de privacidade (E50[39]). Dito isso, é possível solucionar o problema através da elaboração

transparente dos termos de uso, bem como por meio da revisão das bases legais, a fim de que possibilite a criação de uma política de segurança eficaz e atualizada (E43[7]), além de técnicas como Third-Party Tracking e API Configurations (E52[16]).

D9) Relacionamento com o usuário: Por meio das legislações vigentes, é concedido ao titular (usualmente usuário de uma aplicação) diversos direitos — como portabilidade, retificação e exclusão de informações — que influenciam ativamente no processamento de seus dados pessoais (E29[80], E33[84]). Através disso, a dificuldade na relação entre o usuário e a organização ou parte dos desenvolvedores foi identificada como um desafio nos estudos, inclusive até mesmo no processo de consentimento, uma vez que há uma parcela de usuários que são indiferentes aos benefícios da privacidade (E43[7], E39[90]). Adicionalmente, existe por parte dos desenvolvedores uma grande dificuldade em implementar transparência — por meio de políticas de privacidade e sistemas de requisição — em software, o que evidencia ainda mais o desafio (E44[93]). Todavia, o estudo proposto por Wiefling et al. (E44[93]) mostrou que renomadas empresas, como Microsoft e Google, já mitigam esse problema, por meio de ferramentas de autoatendimento, ou semelhantemente, os painéis de privacidade.

D10) Priorização de requisitos funcionais: No que tange a priorização de requisitos funcionais por parte dos desenvolvedores, os estudos apontaram uma série de fatores a serem levados em consideração, tais como a redução de desempenho de sistemas (E11[4], E45[94]), os prazos apertados para implementação de segurança efetiva (E29[80]) ou meramente a dificuldade em implementar requisitos não-funcionais (E43[7]). O fato é que há uma tensão identificada entre prioridades (E39[90]) e a priorização de requerimentos funcionais em detrimento da segurança e privacidade e, dessa forma, é considerado um desafio relevante no contexto de conformidade com uma legislação de privacidade (E24[78]). Quando o problema é dado pelo prazo, a aplicação de testes automatizados podem favorecer importância dada aos requisitos não-funcionais e a utilização de métodos que contribuam para uma rápida atualização das aplicações e feedback efetivo podem igualmente motivar os desenvolvedores no aperfeiçoamento de ambas categorias de requisitos (E21[43]).

D11) Incerteza dos processos organizacionais: Quando se trata da relação entre organização e desenvolvedor, é factível que nem sempre o último conhecerá todos os processos organizacionais. Essa relação é ainda mais problemática, uma vez que é necessário que todas as etapas de tratamento dos dados pessoais estejam de acordo com o estabelecido pela legislação vigente, o que motiva em desafios na adequação de backups (E11[4]), no estabelecimento de auditorias de sistemas e processos (E33[84]) e na utilização de serviços em nuvem (E49[60]) (que também dependem do local em que os dados estão fisicamente armazenados). A partir disso, um bom ponto inicial para mitigar os

riscos de incerteza é por meio de registros de acesso, quando se trata do tratamento dos dados, e optar por provedores de nuvem que são compatíveis e garantam a conformidade com as legislações vigentes (E11[4]).

D12) Dificuldades em serviços de terceiros: Alomar et al. (E50[39]) evidenciam que grande parte dos problemas relativos à privacidade são derivados da utilização de kits de desenvolvimento de software de terceiros – Software Development Kits (SDKs). Isso quer dizer que, por mais que uma aplicação tenha sido implementada, nativamente, em conformidade com a legislação vigente, ao adotar SDKs o desenvolvedor não terá a garantia de que a conformidade foi mantida (e comumente empresas sequer analisam esse tipo de contrato e a garantia de conformidade (E40[91])), o que elucida uma nova classe de desafios que abordam até mesmo gerenciamento de processos de contratação (E11[4], E33[84]). Sendo assim, um dos principais desafios apontados pelos desenvolvedores é navegar pelas implicações de privacidade dessas bibliotecas e, do mesmo modo, ainda não é claro como as bibliotecas processarão os dados pessoais (E52[16], E53[98]). Acerca de soluções que tratam do desafio, têm-se que deve haver uma priorização de bibliotecas de provedores proeminentes e, ademais, sempre que possível não compartilhar dados que não sejam absolutamente necessários com terceiros (E53[98]).

D13) Escassez de guias/ferramentas: Como abordado acima que as legislações de privacidade apresentam pontos de ambiguidade e, além disso, é difícil traduzir a legislação para um contexto técnico, guias e ferramentas contribuem para o processo de conformidade. Todavia, a falta de guias específicos para a aplicação da privacidade em contexto de software é um problema evidenciado pelos desenvolvedores brasileiros e europeus (E24[78], E43[7]). Ekambaranathan et al. (E53[98]) identificaram, por meio de entrevistas, que muitos desenvolvedores de aplicativos dispunham de dificuldades em encontrar diretrizes de design adequadas e específicas, além de que quando encontravam, o suporte era insuficiente para empresas menores. Dessa forma, soluções como o enfoque na boa experiência do usuário e a consulta de profissionais, na ausência de guias e ferramentas, foram elucidadas no trabalho.

D14) Processamento de dados internacionais: No que tange às organizações que tratam dados de pessoas globalmente, um desafio acerca de qual legislação vigente priorizar é identificado (E13[15]). Como tratado na RQ.1, as leis possuem muitos pontos de divergência entre si, o que podem ocasionar em expectativas de resposta judicial e dificuldades contratuais, principalmente quando se trata de pequenas e médias empresas (E13[15], E40[91]). É evidente que todos os demais desafios são somados a esse, uma vez que se deve estabelecer uma solução em comum para as dificuldades de garantir a conformidade com as múltiplas leis. De modo prático, um bom ponto de começo é o mapeamento e posterior análise do fluxo de dados (E13[15]), além de que o uso de

ferramentas e automação pode facilitar o processo de conformidade técnica.

D15) Mudanças nos estágios de desenvolvimento: No processo de desenvolvimento de um produto, é comum que ocorram mudanças em algum dos estágios, que variam desde crescimento da infraestrutura e dos dados até reajustes de sistemas para torná-los mais compatíveis em determinado aspecto (E10[18], E29[80]). Por mais que essas mudanças sejam, por vezes, necessárias, é fato que aumentam a complexidade técnica e requisitam de reformulações em técnicas que implementam privacidade em software (E29[80]). Li et al. (E21[43]) explanaram o desafio de equilibrar a conformidade com a GDPR em um ambiente de negócios competitivo de dados e, a partir disso, uma solução apontada no estudo é a utilização de engenharia de software contínua, dado que une rápidas atualizações e feedback, e possibilita a correção acelerada de pontos de não conformidade (identificados no feedback).

D16) Trade-off ética x economia: É um entrave que qualquer organização em atuação encontrará é encontrar o ponto de equilíbrio entre o respeito à privacidade e a priorização da liberdade corporativa (E5[38]). Uma vez que o objetivo primário de uma empresa é econômico, dada pela natureza do negócio (E29[80]), o enfoque na privacidade e proteção dos dados pessoais pode ser colocado em agenda de baixa prioridade (E6[67]), mesmo que existam leis que exijam a conformidade. Rocha et al. (E43[7]) mostraram que as organizações devem considerar, no plano econômico, as possíveis sanções administrativas em caso de não conformidade com as legislações e que a redução de confiabilidade por parte dos clientes ocasiona desvantagem competitiva a longo prazo, o que pode vir a acarretar em prejuízos financeiros da organização.

D17) Identificação de requisitos de privacidade: Como abordado anteriormente, os desenvolvedores possuem um conhecimento empírico a respeito da privacidade, mas identificar requisitos de privacidade de uma aplicação, em função de uma legislação de proteção de dados, é um trabalho complexo (E38[89]). Assim, faz-se necessário um artifício para auxiliar na conformidade com a lei vigente, como por exemplo, a especificação de Histórias de usuário, a fim de facilitar a etapa de análise de requisitos (E10[18]). Ademais, como técnica empregada em equipes ágeis, uma possível solução seria a utilização de ferramentas de Design Thinking na etapa de elicitação de requisitos (E9[69]), de mesmo intuito.

D18) Impacto na usabilidade da aplicação: Trata-se de um problema relativo à pequenas e médias empresas, uma vez que caso o poder de processamento dos dados não seja o suficiente, a adição de um arcabouço de privacidade e proteção de dados pode vir a reduzir o desempenho do sistema ou inviabilizar a utilização de uma aplicação (E34[85]). É recomendado o emprego de frameworks específicos tão antes quanto possível, isto é, no processo de design da aplicação (E34[85]), a fim de estimar e evitar riscos de performance.

RQ.2 Summary: Os principais desafios para a garantia da conformidade estão relacionados com o processo de entendimento da lei. Uma massiva quantidade de desenvolvedores e organizações ainda possuem dificuldade em compreender a teoria da legislação e como aplicá-la em um contexto técnico. Restrições impostas pelas organizações e falta de material adequado para auxiliar na implementação da privacidade em software por parte dos desenvolvedores também foram identificados como grandes desafios.

3.7 Síntese deste Capítulo

Este capítulo elucidou o processo utilizado para conduzir a RSL, bem como os resultados desta revisão. Os resultados resumidos foram apresentados nas Tabelas 3.7 e 3.8, com as comparações das leis e desafios em obter conformidade, respectivamente. A string de busca retornou um total de 687 estudos e, após a aplicação dos critérios de inclusão e exclusão (tanto pelo resumo, quanto pela leitura do artigo completo) foram selecionados 15 estudos. A partir disso, o processo de snowball foi realizado e possibilitou a identificação de 38 novos estudos (por meio de 7 iterações até a saturação), sendo 53 no total. Esses artigos revelaram que apesar de semelhanças em relação ao escopo das legislações, a GDPR se destacou como sendo a de maior impacto na proteção de dados pessoais e, em contrapartida, a lei australiana carece de reformulações para garantia da privacidade — como ocorre na União Europeia — em meio digital. Não só isso, mas o principal desafio para que as organizações possam atingir a conformidade com as leis foi em compreender as diretrizes das mesmas e, consequentemente, saber aplicá-las em um contexto técnico.

Capítulo 4

Validação dos Desafios — Survey

Neste capítulo está detalhado o questionário aplicado para validar os resultados obtidos pela Revisão Sistemática de Literatura (RSL), quanto à questão dos desafios (RQ.2), para o contexto dos desenvolvedores brasileiros. Há disposição da configuração, da elaboração e dos resultados do survey.

4.1 Configuração do Survey

O survey foi desenvolvido por meio da plataforma Google Forms e o tempo estipulado para leitura e preenchimento foi de aproximadamente 8 minutos, dado que não é necessário pesquisar informações avulsas (há breve explicação dos desafios no próprio survey). Inicialmente, os participantes foram convidados individualmente através da plataforma LinkedIn, a fim de que houvesse priorização na seleção de participantes que atuam na área de desenvolvimento de software e fossem familiarizados com a Lei Geral de Proteção de Dados (LGPD). Adicionalmente, o survey foi divulgado em outras redes sociais, com o intuito de satisfazer a condição da análise quantitativa.

Os respondentes foram informados que a participação é anônima, voluntária e meramente para fins de pesquisa, de modo que deveriam consentir em participar da pesquisa. Além disso, o processo poderia ser interrompido a qualquer momento, sem penalidade e sem registro parcial dessas informações. Por fim, o e-mail institucional do autor foi disponibilizado com o intuito de sanar quaisquer dificuldades que os respondentes encontrassem durante o survey.

4.2 Elaboração do Survey

O questionário contém questões quanto ao perfil do participante, isto é, trata de categorizar o respondente quanto à experiência acadêmica e profissional (vide Tabela 4.1).

Além disso, também apresenta na Tabela 4.2 questionamentos que buscam validar os desafios identificados na Revisão Sistemática de Literatura — Subseção 3.6.2 — quanto aos desafios apresentados pelos desenvolvedores de software e suas respectivas organizações. Assim, para facilitar a visualização, uma cópia da esquematização do survey — além das respostas discutidas posteriormente — pode ser encontrada no repositório da plataforma Zenodo [66].

Tabela 4.1: Perguntas relativas ao perfil do participante.

ID	Pergunta	Escala de resposta
Q1	Qual a sua faixa etária?	Menor de 21 anos; entre 21 e 25 anos; entre 26 e 30 anos; entre 31 e 35 anos; entre 36 e 40 anos; entre 41 e 45 anos; entre 46 e 50 anos; entre 51 e 55 anos; entre 56 e 60 anos; mais de 60 anos.
Q2	Em qual Estado você mora?	AC; AL; AP; AM; BA; CE; DF; ES; GO; MA; MT; MS; MG; PA; PB; PR; PE; PI; RJ; RN; RS; RO; RR; SC; SP; SE; TO.
Q3	Qual é seu nível de escolaridade?	Graduando; graduado; especialização; mestrado; doutorado.
Q4	Em qual etapa de desenvolvimento de software você atua profissionalmente?	Elicitação de requisitos; análise de dados; modelagem de sistemas; desenvolvimento/programação; testes; manutenção e evolução de software; outro.
Q5	Qual é a natureza da organização em que você trabalha?	Empresa privada; Agência da Administração Pública Federal; Projeto de pesquisa/colaboração; Empresa estatal (BB, CEF, SERPRO, DATAPREV); Projeto de software de código aberto; Autônomo.
Q6	Há quanto tempo você trabalha com desenvolvimento de software?	Menos de 1 ano; entre 1 e 3 anos; entre 4 e 6 anos; entre 7 e 9 anos; entre 10 e 15 anos; mais de 16 anos.
Q7	Em relação a questão de privacidade de dados, você tem familiaridade/conhecimento da Lei Geral de Proteção de Dados (LGPD).	Escala Likert (Concordo totalmente; concordo; não concordo, nem discordo; discordo; discordo totalmente).

De Q1 até Q7, os respondentes são questionados acerca de seus perfis e devem selecionar entre as opções pré-definidas, uma vez que se busca identificar e categorizar o participante quanto à experiência prévia. Ademais, Q7 procura constatar se há conhecimento prévio acerca da LGPD, a fim de contrastar com o principal desafio (D1) encontrado na RSL.

Tabela 4.2: Perguntas relativas aos desafios dos participantes.

ID	Pergunta	Escala de resposta
Q8	Assinale quais dos desafios elencados abaixo você enfrenta na sua organização para garantir a conformidade com as legislações de privacidade.	Caixas de seleção.
Q9	Em sua opinião, quais são os maiores desafios para implementar os princípios da LGPD durante o desenvolvimento de um software?	Em aberto.
Q10	Em sua opinião, quais são as melhores técnicas/práticas que garantem a privacidade e a proteção de dados exigidas pela LGPD?	Em aberto.
Q11	Você poderia nos descrever em detalhes como a sua equipe mitiga os desafios para estar em conformidade com a LGPD?	Em aberto.
Q12	Caso tenha algo a acrescentar, por favor use esta questão.	Em aberto.

Na questão Q8 há 19 alternativas em caixas de seleção, que correspondem aos 18 desafios abordados na Tabela 3.8 e, adicionalmente, uma alternativa em aberto que o respondente pode adicionar um desafio não abordado no survey, caso ele deseje. Para cada

declaração, o respondente deve marcar a alternativa se o respectivo desafio é presente em sua organização, a fim de que as classes dos desafios possam ser recondicionadas para o contexto brasileiro. As alternativas de Q8 são identificadas e enumeradas abaixo:

(QD1) Escassez de conhecimento da lei: Falta de conscientização sobre a importância de incorporar medidas de privacidade nos softwares desenvolvidos ou a falta de conhecimento teórico sobre os requisitos legais propostos na lei.

(QD2) Traduzir a lei para um contexto técnico: Dificuldade em interpretar normas predominantemente teóricas, sem diretrizes técnicas específicas, o que torna complexa a adaptação dos requisitos legais para a implementação de medidas de privacidade em softwares.

(QD3) Restrições de orçamento: A privacidade é afetada pois o processo de conformidade com a lei é caro e demorado, e os recursos humanos e financeiros são limitados.

(QD4) Falta equipe com expertise: Falta de um Encarregado pela Proteção de Dados (DPO) com conhecimento teórico abrangente.

(QD5) Estrutura organizacional: Comunicação insuficiente entre especialistas em privacidade e desenvolvedores de software, resultando na implementação inadequada de medidas de privacidade nas aplicações.

(QD6) Ambiguidade da lei: Requisitos não são expressos de forma simples e específica, logo estão sujeitos a várias interpretações.

(QD7) Falta padronização de técnicas/ferramentas: As legislações não fornecem orientações específicas sobre tecnologias a serem utilizadas, deixando as organizações responsáveis por obter um consenso há consenso na definição e avaliação da privacidade.

(QD8) Falta política de segurança/privacidade: Falta termos de consentimento claros e políticas de segurança, como procedimentos de notificação em caso de violação de dados.

(QD9) Relacionamento com o usuário: Direitos concedidos aos titulares de dados pelas legislações, como portabilidade e exclusão de informações, dificultam os procedimentos da organização.

(QD10) Priorização de requisitos funcionais: Fatores como prazos apertados e dificuldades em implementar requisitos não funcionais, por exemplo, são motivações comuns de não implementação de requisitos não funcionais.

(QD11) Incerteza dos processos organizacionais: Não há conhecimento do desenvolvedor como alguns processos são realizados, como backups e auditorias de sistema, mas somente parte deles.

(QD12) Dificuldades em serviços de terceiros: Incerteza quanto à garantia da conformidade com a lei ao utilizar kits de desenvolvimento de software (SDKs) e serviços de terceiros.

(QD13) Escassez de guias/ferramentas: Dificuldade em encontrar diretrizes de design adequadas e específicas, e quando encontram, o suporte muitas vezes é insuficiente para empresas menores.

(QD14) Processamento de dados internacionais: Dificuldade em garantir a conformidade com as múltiplas leis de privacidade para organizações que lidam com dados de usuários globais e quais devem ser priorizadas.

(QD15) Mudanças nos estágios de desenvolvimento: Constantes mudanças em software, que geram aumento da complexidade técnica e exigem reformulações nas técnicas de implementação de privacidade.

(QD16) Trade-off ética X economia: Dificuldade em encontrar um equilíbrio entre respeitar a privacidade e priorizar a liberdade corporativa.

(QD17) Identificação de requisitos de privacidade: Conhecimento empírico sobre a privacidade mas dificuldade em elicitar requisitos de privacidade que apresentam conformidade com a legislação.

(QD18) Impacto na usabilidade da aplicação: A adição de um arcabouço de privacidade e proteção de dados pode diminuir o desempenho do sistema ou tornar a aplicação inutilizável se o poder de processamento dos dados não for suficiente.

(QD19) Outro(s).

Além disso, a questão Q9 busca identificar novos desafios não elucidados pela RSL, especificá-los nas classes existentes (D1 até D18) e, caso necessário, criar novas classes. Assim, a resposta à essa questão é aberta, uma vez que a categorização é feita por meio de Teoria Fundamentada [29]. Em seguida, a questão Q10 busca identificar as técnicas que os desenvolvedores consideram importantes para garantir a privacidade e proteção de dados à nível LGPD. Isso quer dizer que, além das ferramentas e técnicas identificadas na RSL, a questão tem o intuito de averiguar os métodos preferidos dos desenvolvedores brasileiros. Na questão Q11, semelhantemente, busca-se explicitar o processo de solução

dos desafios para alcançar a conformidade com a LGPD. Por fim, a questão Q12 é um espaço em aberto aos respondentes, a fim de que possam opinar a respeito da estruturação do questionário ou acerca de uma pergunta específica.

4.3 Resultados do Survey

Os resultados e discussões do questionário são destacados em subseções, a fim de proporcionar uma visualização facilitada dos dados coletados. Dessa forma, as seguintes subseções e descrições das mesmas são elencadas: 4.3.1, em que são apresentados os dados referentes ao perfil dos participantes; 4.3.2, em que há averiguação dos desafios encontrados pelos desenvolvedores brasileiros em contraste com os obtidos na RSL, identificação de novos desafios e as técnicas utilizadas pelos desenvolvedores para garantir a conformidade com a LGPD, isto é, para mitigar os desafios identificados.

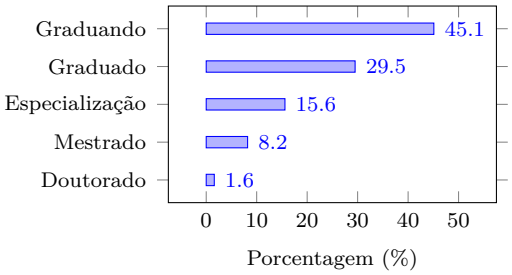
4.3.1 Informações Demográficas

O survey ficou disponível por 41 dias (entre maio e junho de 2024) e foram obtidas 122 respostas, de modo que para realizar o perfilamento do participante, foi utilizada análise de frequência nas perguntas da Tabela 4.1 e os resultados estão apresentados na Figura 4.1. Assim, foram identificados respondentes que variam em oito etapas de desenvolvimento de software, dez Estados e seis categorias de organização, como mostrado nas Figuras 4.1c, 4.1d e 4.1e.

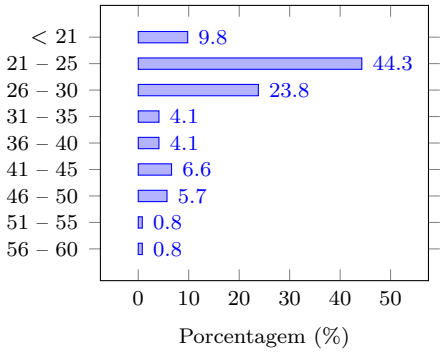
Para realizar um mapeamento inicial, os participantes foram divididos em nível de escolaridade e faixa etária, de modo que: uma maior parcela dos respondentes era estudante de graduação (45,1%), todavia, em uma visão ampla, 54,9% possuía uma graduação ou pós-graduação (vide Figura 4.1a); e uma parte expressiva dos participantes (44,3%) encontra-se na faixa de 21–25 anos e, considerando um pequeno aumento no intervalo, quase 70% está entre 21–30 anos (vide Figura 4.1b).

Com relação às etapas de desenvolvimento de software em que os participantes atuavam, foram definidas inicialmente seis, além da possibilidade do respondente inserir uma área que não foi contemplada pelas alternativas do survey. Logo, foi necessária a criação de duas categorias e suas respectivas áreas: Operações de TI, em que são contempladas áreas como infraestrutura, produção, consultoria e gestão; e Arquitetura de software, com ênfase na arquitetura em si e na engenharia de sistemas. Assim, a maior parcela dos participantes (63,9%) atua na parte de desenvolvimento — programação — de software (vide Figura 4.1c).

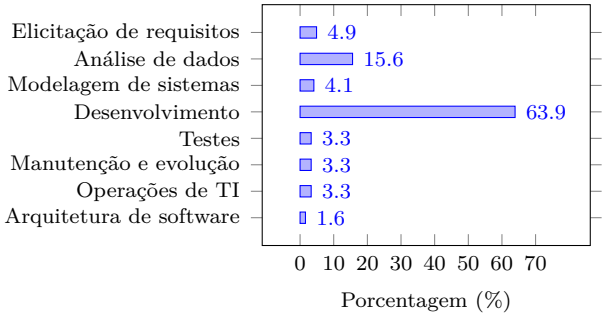
Acerca da localidade e origem da organização, quase três-quartos (72,1%) dos respondentes residem no Distrito Federal (DF) (vide Figura 4.1d) e a maioria (60,7%) é



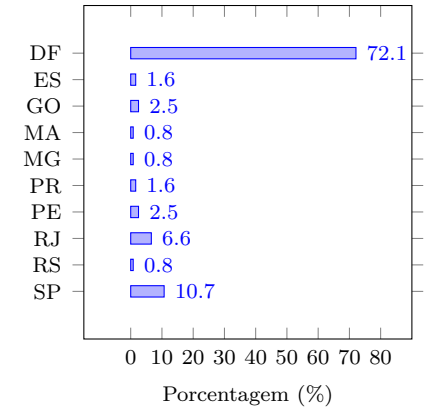
(a) Nível de escolaridade.



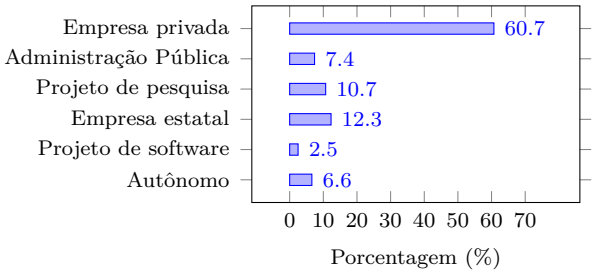
(b) Faixa etária.



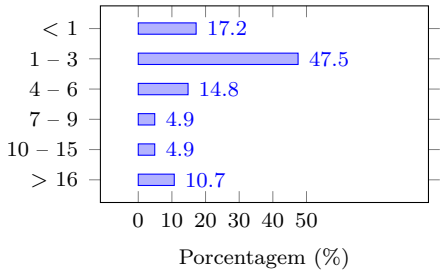
(c) Área de trabalho.



(d) Estado.



(e) Natureza da organização.



(f) Experiência.

Figura 4.1: Perfil do participante: dados demográficos.

empregado em empresa de origem privada (vide Figura 4.1e). Já com relação à experiência profissional no atual trabalho, quase metade (47,5%) dos participantes apresenta de 1–3 anos e há somente 35,3% com mais de 3 anos de experiência (vide Figura 4.1f). Essa informação em conjunto com o nível de escolaridade e a faixa etária corroboram com a hipótese de que há uma parcela significativa de participantes que ingressaram há pouco tempo no meio profissional.

Os respondentes também foram motivados à expressar suas opiniões acerca da familiaridade com a LGPD, a fim de contribuir para a estruturação do perfil dos participantes. Desse modo, 80% dos participantes concordaram que já possuíam familiaridade ou conheciam a LGPD, e apenas 3% definitivamente não (vide Figura 4.2).

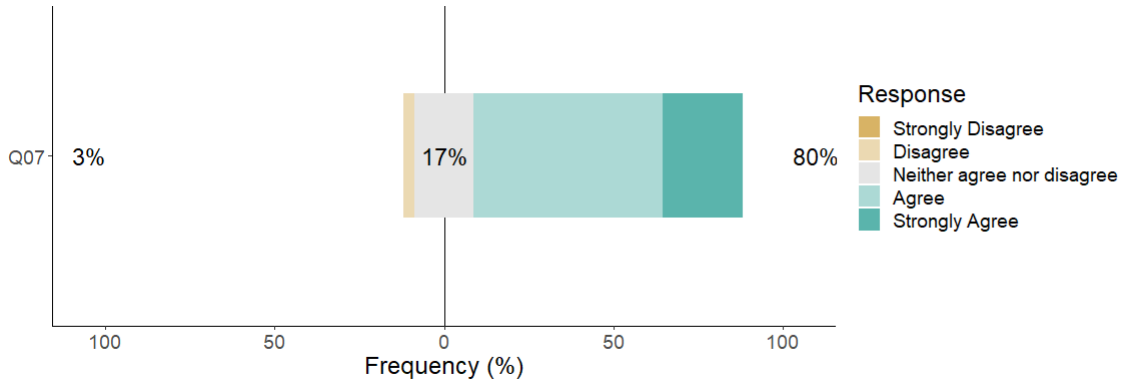


Figura 4.2: Perfil do participante: familiaridade com a LGPD.

4.3.2 Desafios de Conformidade e Técnicas de Mitigação (RQ.2)

Para a análise das respostas de texto livre (Q9 até Q12), foi adotado o processo de Teoria Fundamentada evoluída [29], que é aplicado a partir das seguintes etapas e suas respectivas descrições:

1. Coleta dos dados: A partir da RSL, com os principais desafios de implementação das leis de proteção de dados já identificados, o survey proposto teve o intuito de validar e identificar novos desafios e técnicas. Dessa forma, a coleta de dados não apresentava inicialmente hipóteses pré-definidas, uma vez que o objetivo é explorar os desafios e técnicas de forma aberta, a fim de descobrir novos padrões.

2. Codificação Aberta: Foi realizada uma análise linha por linha das respostas, com o intuito de segmentá-las e categorizá-las, isto é, relacioná-las com os padrões identificados na RSL. Em caso da inexistência desses padrões, foi criada uma nova categoria para o desafio.

3. Codificação Axial: Após a elaboração das categorias, que em grande parte já haviam sido definidas na RSL, foi realizada a análise de como as técnicas explanadas pelos respondentes condiziam com os desafios apresentados, com o intuito de quantificar e classificar os mesmos. Para isso, as maiores técnicas e artifícios de mitigação dos desafios (Q10 e Q11) foram tidos como referência para solução dos respectivos desafios (Q9) de cada respondente.

4. Codificação Seletiva: Foi realizada uma análise mais focada nas categorias centrais que emergiram das fases anteriores. A partir dessas categorias, procurou-se entender como as técnicas de mitigação estavam conectadas aos desafios mais recorrentes, com o objetivo de refinar e selecionar as categorias mais relevantes (dificuldades em compreender a lei e a traduzi-la para um contexto técnico, por exemplo). Sendo assim, houve enfoque na síntese das informações e a identificação de padrões-chave para a construção da teoria final.

5. Teoria Fundamentada: Com base nas categorias já refinadas, foi possível desenvolver uma teoria fundamentada que explica os desafios enfrentados pelos desenvolvedores na implementação da LGPD, inclusive os novos desafios identificados. Essa teoria foi construída a partir dos dados coletados, de modo a refletir as relações entre os desafios e as soluções propostas pelos participantes, além de fornecer uma explicação dos padrões emergentes que surgiram no estudo.

Os resultados acerca dos desafios são expostos na Figura 4.3 e é importante observar que os participantes sugeriram três desafios, até então, não elucidados pela RSL, que são: constantes mudanças na lei; processo de desenvolvimento não avaliado conforme requerido pela LGPD; e projetos criados sem privacidade por padrão (*Privacy by Default*).

Para a apresentação dos desafios (inclusive os abordados em Q9) e suas respectivas técnicas de mitigação (Q10 e Q11), foi utilizada a categorização dos mesmos em três partes: desafios da legislação, em que são consideradas as dificuldades que têm origem na própria lei (QD1, QD2, QD6 e QN3); desafios das organizações, em que são relatadas as dificuldades que as empresas possuem maior potencial de impacto (QD3, QD4, QD5, QD8, QD9, QD10, QD11, QD15, QD16 e QN1); e desafios dos desenvolvedores, em que as dificuldades encontradas possuem uma relação dependente de quem implementa a privacidade (QD7, QD12, QD13, QD14, QD17, QD18, QN2).

Desafios da Legislação e suas Técnicas

Os resultados da Figura 4.3 apontam que a maior dificuldade dos desenvolvedores brasileiros — 50,8% — foi a de escassez de conhecimento da lei (QD1), semelhantemente ao encontrado na RSL. Assim como proposto pelo trabalho de Aljeraisy et al. [25], o desafio é oriundo — majoritariamente — pela falta de conscientização dos desenvolvedores da privacidade em software. Além da escassez de informações precisas de como a LGPD afeta o desenvolvimento de software, mais da metade dos participantes apontaram como maior desafio a leitura e compreensão da lei, como elucidado pela transcrição de um dos respondentes:

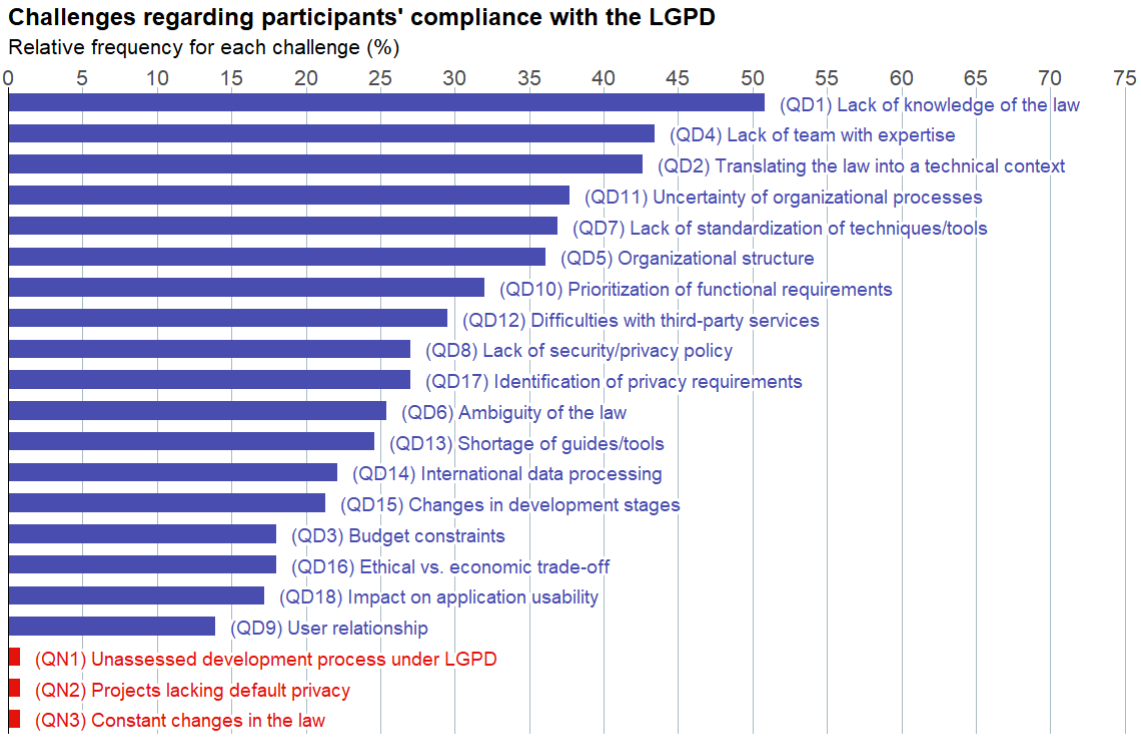


Figura 4.3: Relação dos desafios apresentados pelos participantes.

> "A complexidade jurídica atrelada a LGPD, que muitas vezes são de difícil entendimento para desenvolvedores sem conhecimento especializado na área de direito. Algo que talvez poderia ser mitigado com programas de treinamento."

Como supracitado, programas de treinamento especializado e educação contínua para os desenvolvedores da equipe é o grande pilar para assegurar a conformidade com a lei e edificar a cultura de privacidade na organização. Em maior nível de detalhamento, o ponto-chave elucidado para solucionar esse desafio (tanto na RSL, quanto no questionário) é uma boa política de governança, com treinamento regular para funcionários — principalmente os novos — acerca de práticas corretas de manuseio de dados e as obrigações da LGPD.

Além da problemática que é compreender a teoria da LGPD, os respondentes indicaram que a tradução da lei para um contexto técnico (QD2) também é um problema complexo. 42,6% dos participantes apresentaram dificuldades na implementação da privacidade em software, como mostrado na Figura 4.3, mesmo que amparados pelas técnicas propostas pela LGPD. Assim como elucidado na RSL, grande parte dos desenvolvedores consideram um desafio correlacionar o artigo teórico com decisões práticas rotineiras, isto é, falta uma noção exata do que é necessário ser extraído da lei e implementado em soft-

ware. Não só isso, mas também o processo de anonimização é de extrema complexidade para os desenvolvedores, visto que foi informado que falta clareza de quais dados devem ser anonimizados e há carência de exemplos práticos.

A utilização de frameworks, como Privacy by Design e do princípio de privacidade por padrão (Privacy by Default) foi recomendado por parte dos respondentes, do mesmo modo que na RSL [4]. Todavia, um ponto de destaque para o survey é que diversos desenvolvedores apresentaram técnicas de mitigação, com origem na análise da base de dados. Assim, para analisar quais dados são necessários uma maior cautela, foi indicada a utilização de uma Política de Classificação da Informação, para então realizar a catalogação e rotulação dos dados. Diversas ferramentas *open source* foram recomendadas para essa função, como Openmetadata, Datahub e Amudsen, além de ferramentas para análise dos dados, como Lakeformation e Athena, ambos da renomada Amazon Web Services (AWS). Por fim, também é relevante planejar estratégias de proteção — como medidas criptográficas — e descarte dessas informações, como requisitado pela LGPD por meio do direito de exclusão (Art. 18° [12]).

Um desafio que foi considerado mais problemático na RSL do que no questionário foi o de ambiguidade da lei (QD6), apontado por apenas 25,4% dos respondentes, vide Figura 4.3. A maior dificuldade dos desenvolvedores foi quanto à definição de dados pessoais e sensíveis (Art. 5° [12]), uma vez que é apresentado um escopo abrangente e pouco específico sobre as mesmas. A partir de uma definição ambígua — pela perspectiva dos desenvolvedores — há possibilidade de tratamento inadequado dessas informações internamente e, por conta disso, a reforma legislativa é almejada por parte dos respondentes.

Uma vez que a emenda da lei para evitar casos de ambiguidade dificilmente seria uma solução imediata, a melhor opção é utilizar a tática de prevenção para quaisquer conjuntos de dados. Isso significa que, a técnica de minimização de dados — coletar a menor quantidade de dados possíveis para atingir o objetivo do tratamento — aliada ao mascaramento e criptografia de todos os dados é um método eficaz para mitigação de danos em caso de violação. Além de técnicas orientadas ao pior caso (vazamento das informações), como elucidado pela RSL, os respondentes adicionaram a importância de debates — focalizados no aprendizado — com pessoas internas da empresa que apresentam um maior nível de conhecimento a respeito da LGPD.

Em relação ao novo desafio identificado pelo survey, que se trata das constantes mudanças da lei (QN3), o respondente problematizou a necessidade de manter o software sempre atualizado com as novas regulamentações, quando é necessário seguir múltiplas diretrizes para transferências internacionais dos dados. Uma vez que é requisitado estar em conformidade com diversas legislações — problema de alta complexidade [4] —, o mapeamento e o acesso dos dados coletados devem ser ainda mais rigorosos, além de que

a documentação do software deve conter todas as alterações, mesmo que recentes.

A partir desse problema, uma técnica recomendada por um desenvolvedor é que a organização possua um eficaz Plano de Resposta a Incidentes (PRI), de modo que qualquer alteração na legislação que ainda não foi adaptada em software possa gerar o mínimo de dano possível. Além disso, é trivial que o software esteja sempre atualizado e a documentação do projeto esteja em dia, que pode estar aliada a um processo de versionamento.

Desafios das Organizações e suas Técnicas

Com relação as dificuldades que envolvem as organizações como principal origem, o maior desafio foi o de falta de equipe com expertise em legislações de privacidade (QD4), elucidado por 43,4% dos participantes (Figura 4.3). A maior parte dos respondentes que consideraram esse desafio, afirma que não são todas as organizações que possuem uma equipe especializada na interpretação da LGPD, uma vez que, por ser um conjunto de diretrizes relativamente recente, muitas empresas ainda estão se adequando à essa realidade. Assim como exposto por Ferrão et al. [87], diversos participantes relataram que a falta de suporte nessa área teórica da privacidade ocasiona em falhas na implementação, podendo escalar para possíveis violação dos dados pessoais. A transcrição de um dos respondentes exalta esse tipo de desafio:

> "É extremamente raro que um grupo de desenvolvedores tenha uma pessoa responsável por garantir que a LGPD está sendo seguida corretamente ao longo de todo o processo. Sem uma pessoa responsável, o sistema inteiro fica comprometido pois poucos entendem de fato todas as normas da LGPD."

A solução mais trivial apresentada, é a designação de um encarregado pela proteção dos dados dentro da organização [87], ou a contratação de uma consultoria especializada e até mesmo equipes jurídicas para validar a conformidade com a lei. Todavia, os participantes também expuseram outras técnicas que podem vir a contribuir, em caso de impossibilidade de contratação de uma nova equipe para a organização. Em uma delas — aliada ao desafio QD1 —, é recomendado o treinamento contínuo e conscientização da própria equipe que manipula os dados, uma vez que é ela que realiza o mapeamento e tratamento dos mesmos, a fim de preencher lacunas de expertise. Outra sugestão criativa é a detecção automática de dados sensíveis (por meio de Processamento de Linguagem Natural, por exemplo), durante o tratamento, e advertir aos responsáveis que há uma potencial falha, de modo que essa técnica preventiva não necessariamente requer conhecimento prévio da equipe em legislações.

O desafio que apresentou a maior divergência entre a RSL e o survey foi o de restrições de orçamento (QD3), de modo que os estudos apontaram ser a terceira maior dificuldade das organizações, porém apenas 18% dos participantes do questionário concordaram, como

mostra a Figura 4.3. A partir do que foi relatado pelos respondentes, é um desafio intimamente relacionado ao de priorização de requisitos funcionais, uma vez que por ser extremamente custoso estar em conformidade com as legislações [95], existem outras prioridades para as organizações, como apresentado na transcrição:

> "Falta de incentivo e de prioridade, tendo em vista que tasks prioritárias são aquelas que irão gerar valor para o cliente e, consequentemente, monetização. Seguir a LGPD para quem está desenvolvendo (não apenas os programadores) qualquer software tem um custo financeiro/tempo muito alto."

A partir da RSL, foi recomendada a utilização de um design proativo de privacidade, a fim de garantir aspectos básicos por um baixo custo. Já no questionário, além de reforçar a ideia que é necessário a otimização da gestão, os respondentes apontaram que a melhor solução é a utilização de ferramentas *open source*, principalmente as mais populares e sólidas em meio profissional (como exemplificado em QD2). Dessa forma, ainda que a organização não consiga aplicar capital direcionado à conformidade com a LGPD, por meio dessas ferramentas é possível mitigar diversos problemas imediatos, até que seja viável um maior investimento nessa área.

O problema da estrutura organizacional (QD5) foi igualmente considerado um grande desafio para as organizações, relatado por 36,1% dos desenvolvedores, vide Figura 4.3. Assim como identificado pela RSL [17], há dificuldade em garantir que todos os sistemas estejam integrados e compatíveis com a LGPD. Ademais, os participantes informaram que se trata de um problema multinível, isto é, além de afetar equipes de uma mesma organização, a dificuldade é escalada quando se trata de filiais, dado que uma filial dificilmente conhecerá em completude os processos de outras. Adicionalmente, como observado na RSL, os desenvolvedores ainda enfrentam problemas de comunicação com os especialistas de privacidade [88], e além disso o inverso também é válido, dada a transcrição:

> "Temos os advogados especializados que ditam as regras sobre o que deve ser feito, porém a verificação interna é fraca. Muitas das vezes é verificado apenas o que é mostrado ao usuário. Os advogados não entendem de código, então eles apenas acreditam na boa índole daqueles que codificaram."

Para mitigação do desafio, os desenvolvedores citaram políticas internas que são focalizadas na interação entre as equipes de Tecnologia da Informação e as demais, como as propostas pela Unidade de Tecnologia da Informação. Além da governança adequada, quando se trata desse excessivo compartilhamento de dados pessoais, é relevante que haja uma limitação de acesso, principalmente para dados sensíveis. Relatórios que dispõem *Row-level security* (RLS) são recomendados para seleção de quais informações serão disponibilizadas, e há inclusive arquiteturas que podem contribuir para esse processo de seleção

—*Medallion Architecture*, da Microsoft — e amenizar o conflito entre desenvolvedores e especialistas de privacidade. Há também como garantir que, mesmo entre filiais, os dados manterão a conformidade com a LGPD, que é por meio da utilização de dados *mockados* pelos desenvolvedores e limitação do acesso ao banco de dados de produção.

A falta de política de segurança e de privacidade (QD8) quase ocupou a mesma colocação de dificuldade (no survey e na RSL), de modo que pouco mais de um quarto — 27% — dos participantes informaram que as organizações não possuíam políticas institucionais claras (Figura 4.3). Dessa forma, os respondentes exemplificaram que é um problema que afeta tanto os desenvolvedores quanto os usuários da aplicação, dado que o termo de consentimento — que integra a política de privacidade — deve ser livre e esclarecido, a fim de facilitar a coleta dos dados e garantir a segurança do usuário. Na SLR foi identificado que as organizações, em sua maioria, não notificam às autoridades em caso de violação dos dados pessoais [91] e, no survey, também foram relatadas algumas falhas na política institucional, como: carência de processo caso o usuário não queira mais prover seus dados (direito à revogação do consentimento) e de acesso aos dados. Para a política de segurança, os respondentes informaram que o maior desafio é saber no início do desenvolvimento quais técnicas (algoritmos) de segurança são eficazes e se garantem a conformidade com a LGPD.

Um bom ponto de partida para iniciar a coleta dos dados é a criação de um termo de consentimento que leva em consideração: os objetivos da coleta, quais dados deverão — ou não — ser coletados e uma estimativa de retenção que evite a recoleta. A partir disso, como descrito em QD6, para elaborar uma política de segurança robusta é necessário minimizar a quantidade de dados coletados, bem como a redução de tempo da retenção dos mesmos. Para garantir a segurança dos dados em si, os desenvolvedores destacaram três pontos essenciais: criptografia na base de dados, anonimização sempre que necessário (se possível, sequer exigir dados sensíveis) e controle de acesso com gerenciamento de permissões. A partir disso, em conjunto com um rigoroso mapeamento dos dados coletados, basta realizar a revisão das políticas internas [7] e avaliar riscos e respostas a incidentes para que a política de segurança seja robusta e esteja em conformidade com a LGPD.

Outro desafio que divergiu em relação à RSL foi o de relacionamento com o usuário (QD9), que foi a menor dificuldade — apenas 13,9%, como mostrado na Figura 4.3 — apresentada pelos desenvolvedores no survey. Como identificado na RSL, a maioria dos usuários não se importam em como seus dados serão utilizados [7], fato que potencialmente simplifica esse desafio. Os desenvolvedores que obtiveram problemas quanto à interação com o usuário afirmaram que há certa dificuldade em gerenciar o que o consumidor quer e o que pode ser oferecido, isto é, é necessário conversar constantemente e pesquisar formas de adaptar o tratamento, para que alcance as finalidades e similarmente considere as

diretrizes da lei.

Assim como especificado na RSL, a solução principal para esse desafio é manter a transparência do tratamento e possibilitar a comunicação facilitada com o usuário, como cita a transcrição:

> "Quando se tem contato com os usuários, como na minha área, é muito importante garantir um espaço seguro para os participantes, mantendo sua identidade anônima e abstrair suas opiniões sobre sistemas e serviços."

Além de permitir a comunicação, como também foi relatado na RSL [93], os respondentes informaram que é benéfico integrar os usuários em todo o processo do tratamento, não só possibilitando a contestação. Isto é, em casos de teste de usabilidade que há necessidade de gravação, por exemplo, é de extrema importância que os participantes saibam de todo o processo, além de consentir.

Acerca da priorização dos requisitos funcionais (QD10), foi um desafio que apresentou maior relevância no survey, de modo que 32% (Figura 4.3) elucidou essa pressão das organizações para entrega dos produtos e negligenciar requisitos éticos e legais. Os respondentes discutiram que, por mais que entendam a necessidade da privacidade em software, os prazos estipulados pela organização são curtos — como mostrado na RSL [80] — e a prioridade é desenvolver funções específicas, sendo difícil convencer uma equipe que a segurança é tão importante quanto os requisitos funcionais. Sendo assim, o maior desafio dos desenvolvedores nesse quesito é o tempo, vide transcrição:

> "Geralmente quando estamos desenvolvendo alguma aplicação, o tempo é escasso e temos várias preocupações antes de a aplicação ao menos ir ao ar, como por exemplo usabilidade, responsividade, escalabilidade, comunicação entre o time e o cliente, retorno financeiro da aplicação e etc... Inserir nesse mundo de obrigações a LGPD acaba soando como um atraso, essa é a realidade."

A principal técnica adotada pela maior parte dos respondentes é a de considerar requisitos de privacidade desde o início do projeto, isto é, desde a elicitação dos requisitos funcionais, para desenvolver uma arquitetura sólida antes de implementar em código. Para isso, foram recomendadas diversas técnicas, como: a utilização do framework Privacy by Design; a construção de componentes arquiteturais reutilizáveis (contribui para melhoria da gestão do tempo em projetos futuros); a utilização de práticas pouco custosas, como SHA256 para criptografia, que tem suporte nativo na maioria das linguagens; a utilização de ferramentas para popular banco de dados com finalidades de teste; e o mapeamento contínuo dos dados pessoais, com as informações encaminhadas para a equipe com expertise na legislação, a fim de garantir a privacidade em tempo de desenvolvimento.

Assim como discutido na problemática da estrutura organizacional, tem-se que a incerteza quanto aos processos organizacionais (QD11) foi uma das maiores dificuldades

dos respondentes do survey, com 37,7% (Figura 4.3). Principalmente quando se trata de software legados, os desenvolvedores não sabem se a privacidade foi adequadamente implementada (ou como foi), de modo que a manutenção é complexa e não é tratada como prioridade. Vale lembrar que, caso apenas um único módulo não esteja em conformidade com a legislação, todo o sistema possui a segurança comprometida [4].

Além dos registros de acesso identificados na RSL como tática de mitigação, os respondentes elencaram que o principal é ter uma boa governança de dados e projetos, com controle de acessos bem definido. A partir de uma centralização dos dados em uma aplicação — evitando o uso de sistemas departamentais — e registro de todas as operações de tratamento, é possível garantir a redução nessa incerteza dos processos organizacionais. Ademais, como vastamente recomendado em outros desafios, a minimização dos dados coletados e a baixa retenção facilita a compreensão dos desenvolvedores de como e de quais dados são utilizados pelo sistema.

Em se tratando de um ambiente que está em constante evolução, aproximadamente um a cada cinco participantes — 21,3%, vide Figura 4.3 — informaram que as mudanças nos estágios de desenvolvimento (QD15) é um desafio contínuo. Assim como especificado na RSL, o problema pode estar relacionado à uma ineficaz elicitação dos requisitos de privacidade [80], de modo que os respondentes informaram que é necessário prever como alterações no software afetarão no âmbito legal. Nesse caso, é especialmente problemático quando há demora para identificação dessa quebra de conformidade, como apontado pela transcrição:

> "[...] acontece ocasionalmente, é quando uma aplicação já está desenvolvida e no review aparecem brechas ou falhas que podem contrariar termos da LGPD que não foram detectados antes, durante o desenvolvimento."

Previamente, os desenvolvedores exaltaram que é importante que todo o projeto esteja com a documentação atualizada e, além disso, é interessante que contenha nas mesmas informações sobre as práticas e processos da LGPD. Por conseguinte, para qualquer alteração em software, é necessário realizar o acompanhamento adequado das leis e, consequentemente, avaliações regulares de impacto. Por meio dessas avaliações, como apontado pela RSL [43], há possibilidade de ajuste contínuo conforme o software evolui. Adicionalmente, alguns participantes relataram que a contratação de uma consultoria de direito especializada pode contribuir para a detecção de súbita inconformidade.

O dilema das organizações entre ética e economia (QD16) ocupou a mesma colocação de dificuldade, tanto na RSL quanto no survey, sendo que 18% dos respondentes (Figura 4.3) apresentam problemas para convencer os *stakeholders* que a priorização da privacidade é necessário e justifica o aumento de custos e tempo de desenvolvimento. Conforme apontado pela RSL, a garantia da privacidade em software é um investimento a longo

prazo, que só será percebido em caso de falta, com violações dos dados pessoais e sanções legais [7]. Como relatado por um dos participantes, esse é um desafio que escala conforme o projeto, isto é, quanto maior a organização, maior é o enfoque na liberdade corporativa, em detrimento da privacidade dos dados. A transcrição aborda justamente a valorização das informações e a gradual perda de transparência do tratamento:

> "Em projetos de larga escala, o maior desafio certamente está no trade-off ética X economia, esses projetos comumente estão vinculados a grandes empresas e essas possuem interesses comerciais sobre os dados dos usuários, de modo que nem sempre é do interesse comercial da empresa divulgar o destino desses dados."

Primeiramente, quando se trata de mitigação desse desafio, vale lembrar que em caso de violação dos dados pessoais, as perdas de uma organização não se restringem apenas ao capital, mas também à reputação (que consequentemente acarreta em mais perda monetária) [7]. Dito isso, como apontado pelos respondentes, é improvável que uma organização atualmente não capitalize com as informações dos usuários. Todavia, é importante que a finalidade que esses dados terão esteja explicitamente apresentada em termos de consentimento, bem como a desvinculação dos indivíduos — sempre que possível — dos dados (anonimização). Por fim, como o titular deve possuir o direito das suas informações, é importante disponibilizar uma plataforma que permite a visualização, a modificação e a exclusão definitiva dos dados, caso requisitado.

Há ainda um novo desafio que foi identificado pelo survey, que é o processo de desenvolvimento não avaliado institucionalmente à luz da LGPD (QN1), em que o participante alegou que é comum uma cultura organizacional não voltada para o atendimento da LGPD. Dessa forma, um dos maiores problemas nesse quesito é a mudança da arquitetura de softwares que já estão em produção, mas não foram concebidos atendendo-se aos requisitos da LGPD.

Como forma de mitigação, a utilização de frameworks já conhecidos na literatura — ou a criação de um novo, que seja padrão — para a garantia de que a LGPD esteja instanciada no início de cada projeto. Além de frameworks, guias também foram indicados para mapeamento dos requisitos impostos pela LGPD, a fim de alinhá-los a uma solução no próprio processo.

Desafios dos Desenvolvedores e suas Técnicas

Para os desafios que apresentam maior indício de responsabilidade dos desenvolvedores, a maior dificuldade encontrada foi a falta de padronização das técnicas e ferramentas (QD7), alcançando mais de um terço — 36,9% — dos participantes, vide Figura 4.3. Assim como apontado por Teixeira et al. em relação a GDPR [95], os respondentes do survey relataram a complexidade em definir quais técnicas e ferramentas deverão ser utilizadas

para cada projeto, visto que a LGPD não deixa especificamente explícito quais tecnologias são necessárias para a conformidade. Além disso, a escolha de um método tende a estar intrinsecamente relacionada à compreensão e interpretação dos desenvolvedores acerca da legislação, de modo que a deficiência de padronização por técnicas que já são conhecidas e validadas pode colocar em risco a segurança e a privacidade do software.

Como o intuito deste trabalho é estabelecer um conjunto de técnicas, identificadas pela RSL e pelo survey, que poderão contribuir para a conformidade com as múltiplas legislações, as diversas formas de mitigação dos desafios — citadas nesse capítulo — poderão ser consideradas para esse problema. À título de exemplo, os respondentes citaram tecnologias que variam desde a segurança — como controle de acesso, criptografia SHA256, anonimização, VPNs privadas e *tokens* — até aquelas focalizadas na coleta dos dados, como gestão de consentimento transparente, minimização de dados e auditorias regulares. Em suma, todos os profissionais destacaram a importância de uma comunicação diária com toda a equipe, assim como ocorre em metodologias ágeis — Scrum —, a fim de que todos os integrantes possam estar a par das tecnologias mais recomendadas e suas particularidades.

Acerca de um desafio que foi considerado mais problemático no survey do que na RSL, tem-se a dificuldade com serviços de terceiros (QD12), assinalado por 29,5% dos respondentes (Figura 4.3). A complexidade relatada pelos desenvolvedores é exatamente a mesma da RSL [91], em que é quase impossível entender como os dados são utilizados, armazenados e se estão protegidos, quando se trata de um software que integra código proveniente de múltiplas empresas. Ademais, como pode haver incompatibilidade das políticas de segurança das empresas, a terceirização nessa área — fábrica de software — pode ocasionar em violações, ainda que a organização contratante tenha, anteriormente, respeitado a LGPD durante todos os processos.

As técnicas exploradas pelos respondentes são preventivas e até mesmo reativas, dado que parte se assemelha às identificadas na RSL, como garantir que todos os fornecedores e parceiros cumpram as normas de proteção de dados e evitar trafegar dados sensíveis e informações que não são essenciais para o processamento. Ademais, o mapeamento do software e dos dados, que contenha a documentação, informações do sistema, códigos de terceiros, informações utilizadas, etc. é de extrema importância nessa etapa, justamente para facilitar a compreensão dos desenvolvedores de como os dados são utilizados e armazenados. A segurança dos dados também tem impacto direto na mitigação desse desafio, visto que as técnicas utilizadas são interessantes para a prevenção durante o compartilhamento das informações com terceiros (criptografia em repouso, em trânsito e em uso). Por fim, protocolos internos para a verificação de integridade e confiabilidade de bibliotecas e softwares de terceiros contribuem adicionalmente para a prevenção de violações.

Em se tratando da escassez de guias e ferramentas (QD13) — 24,6% dos respondentes do survey (Figura 4.3) —, a maior parte dos desenvolvedores brasileiros encontram uma maior carência em guias, e não em ferramentas. Como abordado pela RSL [7], modelos que explicam como deve ser feita de fato a implementação da privacidade em software são complementos necessários para a LGPD, haja vista a falta de técnicas específicas para proteção dos dados. Os desenvolvedores também apontaram a escassez de material do comitê de ética a respeito da LGPD e, por utilizarem materiais direcionados para leis estrangeiras, nem sempre há a confiabilidade em que toda a lei brasileira será assentida, vide transcrição:

> "Acredito que por várias vezes o desenvolvimento é feito muito aquém dos princípios da LGPD. Isso ocorre também por conta de nós termos aprendido etapas de desenvolvimento "globais", que são criadas em outros lugares do mundo e não seguem exatamente o que a LGPD propõe."

As palestras, as auditorias especializadas e a interação com o DPO, além de contribuir para a compreensão da equipe de software sobre boas práticas que são amparadas pela LGPD, são relevantes para suprir a falta de guias direcionados. Todavia, os participantes relataram que ter acesos facilitado a um material informativo sobre a LGPD, com normas e suas respectivas técnicas, é positivo para toda a equipe. Um dos respondentes relatou que videoaulas voltadas para essa área e folhetins seriam de grande suporte, o que pode vir a motivar a gravação das palestras e das auditorias, em caso de dúvida da equipe que desenvolve o software. Essa técnica é ainda mais interessante, visto que questões voltadas à LGPD não são tratadas diariamente pelo time de desenvolvimento, e sim por times de compliance da empresa, logo é indispensável um acesso rápido à essas informações.

Sobre um dos principais desafios que esse trabalho busca resolver, 22,1% dos desenvolvedores, mostrado na Figura 4.3, consideraram o processamento de dados internacionais (QD14) como uma grande dificuldade. Assim como apontado na RSL [15], todos os demais desafios são encontrados nessa etapa, visto que os respondentes — em sua maioria — apresentam dificuldade em compreender a lei brasileira, o que pode ser expandido quando se trata de múltiplas legislações de privacidade. Em específico, um respondente afirmou que é mandatório possuir uma consultoria especializada, que valide o compliance da equipe de software em relação às boas práticas de segurança e privacidade.

Como relatado na etapa da RSL, os respondentes também concordam que por meio de uma boa gestão do fluxo dos dados — mapeamento e análise — é possível facilitar o tratamento dessas informações, todavia é necessário atentar-se ao desafio QD3 (constantes mudanças na lei), visto que o escopo a ser considerado é muito maior. Ademais, para mitigar o desafio, alguns respondentes informaram que utilizam frameworks — principalmente Privacy by Design —, na tentativa de integrar uma proteção global dos da-

dos desde o início do desenvolvimento. Todavia, é interessante realizar uma análise de framework, combinado com as legislações em que se busca obter conformidade, para averiguar o quanto o framework utilizado cobre o escopo de cada uma das legislações. Por fim, em um âmbito de engenharia de rede, soluções que monitoram APIs, firewalls de containers, segurança *Shift Left*, etc. contribuem para a segurança do fluxo de dados e, consequentemente, ajudam a garantir a conformidade com esse fragmento da privacidade nas legislações.

A identificação de requisitos de privacidade (QD17) foi considerada uma grande dificuldade por uma relevante parcela dos respondentes (27%, Figura 4.3), de modo que aparenta ser um problema maior para os desenvolvedores brasileiros do que para os profissionais que lidam com a GDPR [89]. Os desenvolvedores informaram que a etapa de elicitação dos requisitos — funcionais ou não — podem ajudar a implementar uma maior segurança de dados em coordenação com a LGPD. Em contrapartida, um levantamento ineficaz desses requisitos acarreta em problemas tanto na coleta dos dados — seleção de dados desnecessários ao software, que fere o princípio da necessidade — quanto no desenvolvimento, com falhas na segurança e passíveis de sanções administrativas.

As técnicas identificadas no desafio de priorização de requisitos funcionais também podem ser consideradas para mitigação de QD17, principalmente pelo mapeamento do ciclo de vida dos dados pessoais (Inventário de Dados). Por meio disso, os respondentes elucidaram que é possível identificar e documentar todos os dados pessoais e seus fluxos, o que contribui para uma segunda análise acerca do que é realmente necessário para atingir as finalidades do software e o que pode ser descartado. Adicionalmente, a equipe de compliance tende a ser de grande relevância para a mitigação desse desafio, principalmente quando o maior desafio para os desenvolvedores tem origem da parte teórica da lei.

Acerca do desafio que foi considerado de menor complexidade através dos estudos da RSL, o impacto na usabilidade da aplicação (QD18) foi assinalado por 17,2% dos respondentes do survey — Figura 4.3 —, e é considerado o segundo desafio menos problemático. Poucos desenvolvedores especificaram qual é o principal obstáculo, mas foi possível observar que a origem é a mesma em todos os casos: a coleta exacerbada dos dados pessoais. Isso quer dizer que a usabilidade das aplicações só foi impactada negativamente quando foi necessário o processamento de uma quantidade exagerada de dados.

Como o desafio QD18 apresentou uma origem muito perceptível — por meio das respostas dos desenvolvedores —, a principal técnica de mitigação é dada em consequência disso: a minimização da coleta de dados. Através dessa prática, o termo de consentimento dos titulares será ainda mais transparente, além de reduzir o potencial impacto na experiência do usuário do sistema. Dessa forma, a posterior organização, tratamento e limpeza de dados também é facilitada, visto que as informações armazenadas respeitarão

o princípio de necessidade proposto pela LGPD.

Semelhantemente às outras subseções, há também um novo desafio identificado pelo survey, que trata de projetos criados sem privacidade por padrão (Privacy by Default) (QN2), o qual é semelhante à problemática da mudança dos estágios de desenvolvimento, todavia trata-se da falta de consideração da privacidade no período inicial. Dessa forma, as falhas que contrariam a LGPD são percebidas logo no começo do desenvolvimento e podem ser facilmente resolvidas, todavia é sempre desejado preveni-las.

Logo, é recomendado definir as configurações de privacidade mais restritivas como padrão, sem necessidade de intervenção do usuário. Em um aspecto mais amplo, um desenvolvedor recomendou a utilização do framework Privacy by Design, dado que a privacidade por padrão é um dos princípios fundamentais. Assim, integrar a privacidade desde o início do desenvolvimento contribui para garantir que a mesma seja considerada um princípio central do projeto, além de evitar sanções indesejadas e retrabalho.

4.4 Síntese deste Capítulo

Este capítulo apresenta uma pesquisa realizada via Google Forms e divulgada no LinkedIn para desenvolvedores, acerca dos desafios de implementar a LGPD em software e suas técnicas de mitigação. Com 122 respostas coletadas, a principal dificuldade identificada foi a falta de conhecimento sobre a lei, semelhante à obtida na Revisão Sistemática de Literatura (RSL). Além disso, surgiram três novos desafios: a ausência de avaliação institucional dos processos de desenvolvimento à luz da LGPD, a falta de Privacy by Design nos projetos e as mudanças frequentes na legislação.

Capítulo 5

Catálogo da Ferramenta Proposta

Neste capítulo é apresentado o guia elaborado a partir dos resultados da Revisão Sistemática de Literatura (RSL) e do survey referente aos desafios dos desenvolvedores brasileiros.

5.1 Análise de Framework

Para a elaboração da etapa de análise comparativa no guia, a tabela dos resultados de RQ.1, na Seção 3 — Tabela 3.7 —, foi utilizada como ponto de partida, de modo que as informações foram seccionadas em cinco tabelas e preenchidas inicialmente apenas com as informações da RSL. As tabelas criadas e suas respectivas subseções foram: (1) Escopo – escopo pessoal, territorial e material, (2) Definições – dados pessoais e sensíveis, responsáveis pelo processamento e processador dos dados, (3) Sanções administrativas, (4) Princípios, e (5) Direitos individuais.

A partir disso, com o intuito de preencher as lacunas, o método de framework analysis [27] foi adotado e consiste em cinco etapas: (1) Familiarização dos dados, (2) Identificação do framework, (3) Indexação, (4) Mapeamento (gráfico), e (5) Mapeamento e interpretação. As etapas são apresentadas com uma breve descrição na Figura 5.1 e, a aplicação de cada etapa do método de framework analysis no presente trabalho ocorreu da seguinte forma:

1. Familiarização dos dados: Inicialmente, foi realizada a leitura integral das cinco legislações de privacidade, de modo que o comparativo com o Privacy by Design (PbD) e a ISO/IEC 29100 foi adicionado posteriormente ao guia. O processo é particularmente relevante para compreender os termos adotados em cada legislação.

2. Identificação do framework: Após a leitura integral das leis, é requerida a identificação de temas relevantes que estão presentes em todas as legislações. Uma vez que os temas já haviam sido identificados na RSL (vide Tabela 3.7), foi realizada

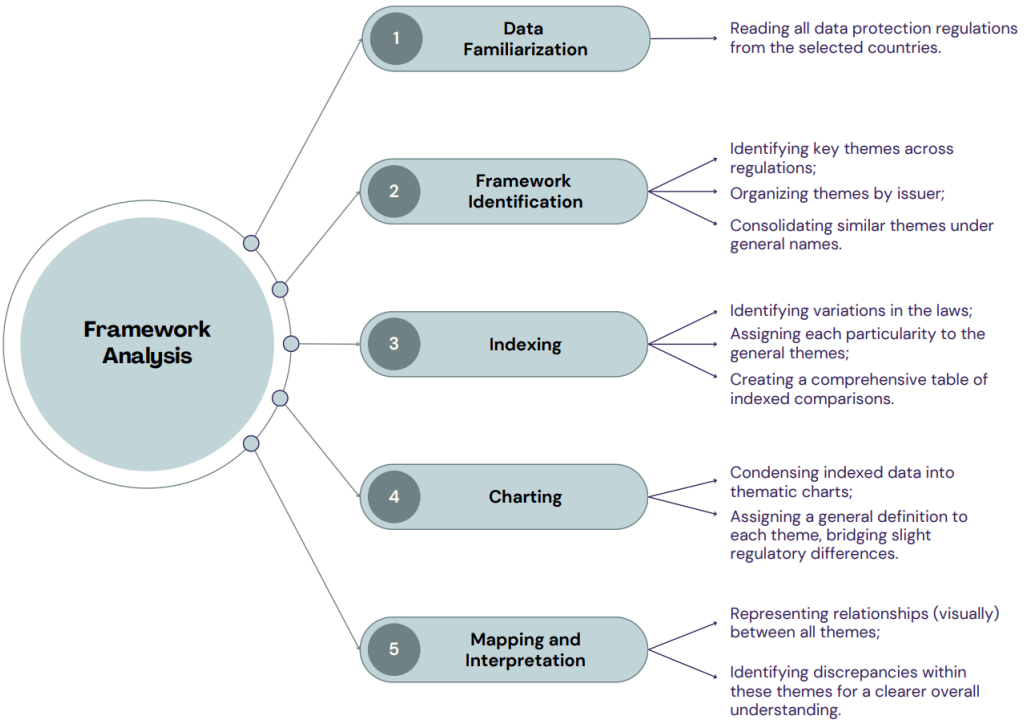


Figura 5.1: Etapas do método de framework analysis [27].

apenas a organização dos mesmos em tabelas distintas, de modo a facilitar a posterior visualização gráfica. Todo o processo foi registrado em uma planilha de dados (Google Sheets), uma vez que se trata de um método relativamente demorado (por requerer a leitura integral de todas as legislações) e é necessário dispor de um acesso rápido e facilitado para cada uma das etapas. Sendo assim, os temas-chave identificados foram: escopo (com subtemas pessoal, territorial e material); definições (com subtemas dados pessoais, dados pessoais sensíveis, responsáveis pelo processamento dos dados; e processador dos dados); sanções administrativas; princípios; e direitos individuais.

3. Indexação: Em seguida, o processo de indexação só se fez necessário na ausência das informações da Tabela 3.7), ou seja, para os temas de princípios e sanções, e adicionalmente para os direitos individuais, uma vez que nem todas as legislações possuem os mesmos direitos. Dessa forma, para esses temas, foi realizada a identificação de suas particularidades nas leis e as mesmas foram ordenadas a partir de um tema geral. Uma vez que o processo envolve questionamentos acerca do quão semelhante ou diferente é uma legislação em relação à outra, também foram elaboradas categorias de semelhança, de modo que:

- ✓ - Y/S: Presente e identificado na revisão da literatura;
- ✓ - Y/O: Presente e identificado diretamente na lei (na mesma seção);
- ✓ - Y/D: Presente em outra seção da lei, mas similar;
- ✓ - Y/C: Presente, mas aplicado a um contexto diferente (requer especificação para aplicação);
- ✕ - N/A: Não encontrado nos artigos ou na lei.

As categorias foram essenciais para a próxima etapa do framework analysis, uma vez que para realizar o processo comparativo de princípios e direitos, foi adotada como base os da Lei Geral de Proteção de Dados (LGPD). Assim, para as outras legislações, houve a adequação de princípios e direitos equivalentes (além de seu nível de equivalência, conforme as categorias).

4. Mapeamento (gráfico): Em seguida, para o processo do mapeamento gráfico, conforme supracitado, foram atribuídas as definições gerais para cada um dos temas. Isso quer dizer que, apesar das particularidades em cada tema para cada legislação, no mapeamento gráfico ocorre um processo de generalização. Embora tal processo não garanta níveis de semelhança entre as leis, as categorias criadas propõem uma forma de classificação, de modo que a generalização não seja binária.

5. Mapeamento e interpretação: Por fim, embora a apresentação dos temas de escopo, definições e sanções sejam meramente textuais, os princípios e definições apresentam um conteúdo massivo, que podem dificultar a interpretação. A fim de reforçar o uso de categorias para comparação desses temas, os mesmos foram mapeados conforme as categoriais e, adicionalmente, comentários foram inseridos na planilha (Google Sheets) do porquê estão inseridos em cada classificação. Todo o processo também foi submetido à uma revisão por três pessoas, a fim de mitigar correlações equivocadas durante a etapa de interpretação.

Dessa forma, a Tabela 5.1 aborda o escopo adotado para cada uma das legislações e, uma vez que trata-se de um trecho correspondente ao da Tabela 3.7, foram adicionadas apenas as informações acerca do consentimento por parte das crianças e acerca dos dados pessoais dos funcionários. Logo, a LGPD e a GDPR seguem semelhantes na questão do escopo, todavia a lei australiana se diferencia na questão da idade mínima para consentimento (não há estabelecido na lei) e por compreender opinião como um dado pessoal. Ademais, a ADPPA se assemelha à CCPA, uma vez que crianças podem consentir a partir de 13 anos.

Tabela 5.1: Comparação do escopo das legislações de proteção de dados.

Tema	LGPD	GDPR	ADPPA	Privacy Act	CCPA
Escopo Pessoal	Consentimento *opt-in*; Enfoque na proteção de dados; Crianças não podem consentir	Consentimento *opt-in*; Enfoque na proteção de dados (grande abrangência); Crianças não podem consentir	Consentimento *opt-out*; Enfoque na liberdade corporativa; Crianças podem consentir a partir de 13 anos	Consentimento *opt-in*; Enfoque na proteção de dados (menor abrangência); Não informa idade mínima para consentimento	Consentimento *opt-out*; Enfoque na liberdade corporativa; Crianças podem consentir a partir de 13 anos
Escopo Territorial	Aplica-se a organizações no Brasil ou fora, desde que trate dados brasileiros	Aplica-se a organizações na U.E ou fora, desde que trate dados europeus	Aplica-se apenas ao processamento de dados de indivíduos residentes dos Estados Unidos	Aplica-se à entidades APP (organizações) que podem ou não estar na Austrália	É aplicada a qualquer entidade com fins lucrativos que faz negócios na Califórnia
Escopo Material	Dado pessoal sensível (associação direta); Compreende dados pessoais de funcionários	Dado pessoal sensível (associação direta e indireta); Compreende dados pessoais de funcionários	Dado pessoal sensível; Não compreende dados pessoais de funcionários	Dado pessoal sensível; Compreende dados pessoais de funcionários; Compreende opinião como dado pessoal	Dado pessoal sensível; Não compreende dados pessoais de funcionários

Com relação às definições, elas foram separadas em subcategorias por meio do framework analysis, apresentando-se de forma diferente da que consta na Tabela 3.7. Como elucidado na Tabela 5.2, houve a criação de temas específicos para as definições, de modo que foram adicionadas às definições os temas de dados pessoais, dados pessoais sensíveis e processador dos dados. Como apontado, todas as legislações apresentam conceitos semelhantes de dados pessoais e dados pessoais sensíveis, todavia há distanciamento quanto ao responsável pelo processamento dos dados. Tanto a LGPD quanto a GDPR apontam uma entidade que desempenha funções semelhantes — do mesmo modo a ADPPA e a CCPA —, todavia não há essa diferenciação entre os responsáveis pelo tratamento na legislação australiana.

Tabela 5.2: Comparação das definições das legislações de proteção de dados.

Tema	LGPD	GDPR	ADPPA	Privacy Act	CCPA
Responsáveis pelo Tratamento	Controlador, operador e encarregado	Controlador, processador e DPO	Entidades cobertas e provedores de serviço	Entidades APP	Negócios e provedores de serviços
Dados Pessoais	Informação relacionada a pessoa natural identificada ou identificável	Informação relativa a uma pessoa singular identificada ou identificável	Covered Data (dados identificáveis de uma pessoa natural)	Qualquer informação sobre um indivíduo mantida por uma agência federal	Informações que identificam, descrevem ou podem ser associadas a um consumidor ou sua família
Dados Sensíveis	Qualquer informação relacionada a uma pessoa identificada ou identificável	Qualquer informação relacionada a uma pessoa identificada ou identificável	Sensitive Covered Data (categorias especiais de dados pessoais)	Qualquer informação sobre um indivíduo mantida por uma agência federal	Informações que identificam, descrevem ou podem ser associadas a um consumidor ou sua família
Processador dos Dados	Operador (entidade que processa dados pessoais em nome do controlador)	Processador (pessoa natural ou jurídica que realiza o tratamento de dados em nome do controlador)	Provedor de serviços (prestador de serviços que processa dados para uma entidade coberta)	Não aplicável (o foco é nas agências federais como controladores)	Provedor de serviços (entidade que processa informações pessoais em nome de um negócio)

Acerca das sanções administrativas, foram adicionadas ao extraído da Tabela 3.7 o período de aplicação das multas, para todas as legislações, além do limite inferior e superior. Além disso, por meio da análise de framework, foi possível preencher a lacuna na lei de privacidade australiana, assim como elucidado na Tabela 5.3. Vale notar que todas as legislações adotam uma política administrativa diferente, exceto a lei australiana, que não apresenta explicitamente as multas administrativas.

Com relação aos princípios e direitos, o mapeamento do framework analysis foi realizado através da categorização de cada. Como base, foram utilizados os dez princípios estabelecidos pela LGPD (Art. 6° [12]) e os direitos individuais explicitados tanto pela

Tabela 5.3: Comparação das sanções administrativas das legislações de proteção de dados.

Tema	LGPD	GDPR	ADPPA	Privacy Act	CCPA
Sanções	Até 2% do faturamento excluídos os tributos (limitado à 50 milhões de reais) ou multa diária de acordo com limite total	Até 20 milhões de euros ou 4% do faturamento total do ano fiscal anterior para violações mais graves, reduzida para até 10 milhões de euros ou 2% do faturamento para violações menores	Sem multas administrativas especificamente definidas, mas organizações que infrinjam o ADPPA ainda podem estar sujeitas a ações de aplicação governamentais e direitos de ação privados	Para interferências graves e repetidas até $2.500.000 para pessoas físicas e até $50.000.000 para pessoas jurídicas, ou três vezes o benefício obtido, ou 30% do faturamento ajustado	De $2.500 a $7.500 dólares por violação e danos estatutários entre 100 e 750 dólares, oferecendo um período de 30 dias para correção.

LGPD, quanto pela GDPR (Capítulo 3 em ambas leis [12], [41]), a fim de massificar esse tema.

A Tabela 5.4 apresenta o framework comparativo entre os princípios das legislações estudadas, de modo que há a indicação de onde o princípio foi identificado, isto é, nos artigos por meio da RSL (Y/S), na própria legislação (Y/O, Y/D ou Y/C) ou se não foi identificado (N/A). A equivalência entre os princípios possuem fundamento teórico, quando identificadas nos artigos, como por exemplo a relação entre o princípio da Finalidade (LGPD) e o *Purpose Limitation* (GDPR) [45].

Dessa forma, para princípios que não possuem uma equivalência direta, foi necessário, por meio do framework analysis, indexar e mapear os mesmos, ainda que houvesse variação da terminologia utilizada em cada legislação. Vale informar que, uma vez que não há uma seção específica para os princípios na ADPPA, nem na CCPA, não há ocorrência da categoria Y/O, isto é, caso em que há princípio na lei e é apresentado na mesma seção (princípios).

A GDPR apresenta a maior parte dos princípios equivalentes à LGPD, como consta na 5.4, todavia existem três que foram identificados em uma outra seção da lei, mas atuam de modo similar aos da LGPD. Os princípio de Livre Acesso, Prevenção e Não Discriminação são considerados direitos individuais pela GDPR, e são equivalentes respectivamente à: *Right of access by the data subject* — Art. 15 —, para Livre Acesso; e *Restrictions* — Art. 23 —, para Prevenção e Não Discriminação [41].

A ADPPA, como discutido no Capítulo 3, foi de difícil identificação na RSL. Ademais, por não possuir seção de princípios, a análise de equivalência é ainda mais complexa. A maioria dos princípios foram associados à *Data Minimization* (SEC. 101 [49]), como Finalidade, Adequação, Necessidade, Prevenção e Não-Discriminação. Ademais, ainda existem princípios que se correlacionam com direitos individuais da lei, tais como Qualidade dos Dados, Transparência e Segurança, sendo respectivamente elucidados na ADPPA por meio dos direitos de correção (*Right of Correction* – SEC. 203), de transparência (*Right of Transparency* – SEC. 202) e de segurança dos dados (*Right of Data Security* – SEC. 208) [49].

Além disso, a ADPPA apresenta correlação com dois princípios da LGPD que são aplicáveis apenas em situações específicas, isto é, para grandes detentores de dados. Os

princípios de Livre Acesso e de Responsabilização são identificados na SEC. 301 [49], e tratam apenas das avaliações de impacto de privacidade para grandes detentores de dados, ou seja, apresentam uma menor abrangência quando comparados com a LGPD e a GDPR.

A lei de privacidade australiana, semelhantemente à GDPR, apresenta um elevado número de princípios que foram identificados na RSL como equivalentes (vide Tabela 5.4). O princípio da Prevenção é garantido por consequência do princípio da Segurança, ou seja, é dado como equivalente à *APP 11–security of personal information* [51]. Todavia, princípios como o de Não Discriminação e Responsabilização não foram identificados, tanto na RSL, quanto no processo de framework analysis.

Por fim, a CCPA também apresenta numerosos princípios equivalentes à LGPD e à GDPR, embora o Livre Acesso seja apresentado na legislação como um direito individual, por meio da seção 1798.110. *Consumers' Right to Know What Personal Information is Being Collected. Right to Access Personal Information* [99]. O princípio de Qualidade dos Dados é apontado, por meio da RSL, como não existente na CCPA [25], já o de Prevenção não foi identificado pelo framework analysis.

Tabela 5.4: Comparação das definições das princípios de proteção de dados.

Princípios	**LGPD**	**GDPR**	**ADPPA**	**Privacy Act**	**CCPA**
Finalidade	✓ Y/S [38],[45],[7]	✓ Y/S [38],[45]	✓ Y/D	✓ Y/S [25]	✓ Y/S [25]
Adequação	✓ Y/S [38],[45],[7]	✓ Y/S [38],[45]	✓ Y/D	✓ Y/S [25]	✓ Y/S [25]
Necessidade	✓ Y/S [38],[45],[7]	✓ Y/S [38],[45]	✓ Y/D	✓ Y/S [25],[50]	✓ Y/S [25]
Livre Acesso	✓ Y/S [38],[45],[7]	✓ Y/D	✓ Y/C	✓ Y/S [25],[50]	✓ Y/D
Qualidade dos Dados	✓ Y/S [38],[45],[7]	✓ Y/S [38],[45]	✓ Y/D	✓ Y/S [25],[50]	✕ N/A
Transparência	✓ Y/S [38],[45],[7]	✓ Y/S [38],[45]	✓ Y/D	✓ Y/S [25],[50]	✓ Y/S [25]
Segurança	✓ Y/S [38],[45],[7]	✓ Y/S [38],[45]	✓ Y/D	✓ Y/S [25]	✓ Y/S [25]
Prevenção	✓ Y/S [38],[45],[7]	✓ Y/D	✓ Y/D	✓ Y/O	✕ N/A
Não Discriminação	✓ Y/S [38],[45],[7]	✓ Y/D	✓ Y/D	✕ N/A	✓ Y/S [25]
Responsabilização	✓ Y/S [38],[45],[7]	✓ Y/S [38],[45]	✓ Y/C	✕ N/A	✓ Y/S [25]

A Tabela 5.5 apresenta, semelhantemente, o framework comparativo entre os direitos das legislações. Para esse tema é interessante observar que na lei australiana — a mais antiga entre as estudadas — não existe de modo exclusivo uma seção para os direitos individuais, de modo que os mesmos são identificados em trechos distintos da lei.

Além disso, para as outras legislações, existem direitos que são considerados princípios (e vice-versa) ou até mesmo em seções excepcionais, como a de Dever de Lealdade (*Duty of Loyalty*) da ADPPA [49]. Vale lembrar que, como a criação do framework dos direitos individuais embasou-se na LGPD e na GDPR, ambas as legislações apresentam a maioria dos direitos já identificados na RSL.

Com relação aos direitos não identificados na RSL para a LGPD, os de Contestação e de Oposição à Tomada de Decisões Automatizadas são identificados na própria seção de direitos, respectivamente nos Art. 18° — §1 e §2 — e Art. 20° [12]. Os direitos de Processamento Consistente com Finalidade e Retenção Consistente com Finalidade podem ser compreendidos em um único princípio, já estabelecido na LGPD, que é o da Finalidade, uma vez que garante que o tratamento será realizado apenas para os propósitos legítimos e sem possibilidade de tratamento posterior de forma incompatível com essas finalidades [12]. Já o direito de Restrição do Processamento é abarcado pela LGPD no Art. 15°, todavia há especificação de situações para que ocorra a restrição (é menos abrangente do que a GDPR).

A GDPR, diferentemente da LGPD, apresenta uma série de direitos que já estão inclusos na seção de princípios, tais como: Coleta Minimizada (Art. 5 – *Data Minimization*), Informação da Possibilidade de Não Consentir (Art. 7 – *Conditions for consent*), Revogação do Consentimento (Art. 7 – *Conditions for consent*), Processamento Consistente com Finalidade (Art. 5 – *Storage limitation*) e Retenção Consistente com Finalidade (Art. 5 – *Storage limitation*) [41]. Além disso, como discutido no Capítulo 2, a GDPR trata o processo de anonimização como *pseudonymization*, como abordado no Art. 4 [41]. Por fim, o direito de Informação das Entidades Participantes é encontrado na mesma seção de direitos, por meio do Art. 13 (*Information to be provided where personal data are collected from the data subject*) [41].

Com relação à ADPPA, poucos direitos foram identificados na RSL, todavia a legislação apresenta uma gama dos mesmos, observados na própria seção de direitos. As prerrogativas de Acesso, Correção e Eliminação dos Dados são todos garantidos por meio da SEC. 203 (*Individual data ownership and control*), enquanto o direito de Informação das Entidades participantes é garantido pela SEC. 202 (*Transparency*) e os direitos de Revogação do Consentimento e Contestação são incluídos na SEC. 204 (*Right to consent and object*) [49].

O direito acerca da Informação da Possibilidade de Não Consentir também é presente na ADPPA, porém existe restrições. O mesmo está incluído na SEC. 202 (*Transparency*), todavia é aplicável em caso de mudança dos termos de consentimento [49]. Dessa forma, seu escopo é mais limitado do que o semelhante apresentado na LGPD e na GDPR. Já em comparação com às outras leis, em contrapartida, a ADPPA apresenta quatro direitos que não foram identificados por meio do framework analysis, conforme apresentados na Tabela 5.5: Confirmação da Existência do Tratamento, Anonimização, Oposição à Tomada de Decisões Automatizadas e Restrição do Processamento.

Para a lei australiana, existem diversos direitos que são garantidos por meio de princípios, uma vez que a mesma não apresenta seção explícita para os direitos individuais.

A correlação entre eles é dada por: Coleta Minimizada (APP 3 – *collection of solicited personal information*); Confirmação da Existência do Tratamento (APP 12 – *access to personal information*); Anonimização (APP 2 – *anonymity and pseudonymity*); Informação das Entidades Participantes (APP 1 – *open and transparent management of personal information*); Revogação do Consentimento (APP 3 – *collection of solicited personal information*/APP 6 – *use or disclosure of personal information*); Processamento Consistente com Finalidade (APP 6 – *use or disclosure of personal information*); Retenção Consistente com Finalidade (APP 11 – *security of personal information*) [51].

Existem ainda um direito que não está relacionado aos princípios na lei australiana, que é o de Acesso aos Dados, referente à seção 20, subdivisão F (*Access to, and correction of, information*). Metade dos direitos não identificados foram elucidados na RSL, que são os direitos de Portabilidade dos Dados, Oposição à Tomada de Decisões Automatizadas e Restrição do Processamento [25]. Os demais direitos (Eliminação dos Dados, Informação da Possibilidade de Não Consentir e Contestação) não foram identificados no processo de framework analysis.

Por fim, a CCPA também apresenta diversos direitos que são encontrados em uma seção explícita de direitos. As prerrogativas de Correção dos Dados, Informação das Entidades Participantes, Informação da Possibilidade de Não Consentir, Processamento Consistente com Finalidade e Restrição de Processamento são equivalentes aos direitos de, respectivamente: *Right to Correct Inaccurate Personal Information*, *Right to Know What Personal Information is Sold or Shared and to Whom*, *Right to Opt Out of Sale or Sharing of Personal Information*, *Right to Know What Personal Information is Being Collected. Right to Access Personal Information* e *Right to Limit Use and Disclosure of Sensitive Personal Information* [99].

A Coleta Minimizada, por sua vez, é equivalente ao *Right to Limit Use and Disclosure of Sensitive Personal Information*, todavia ela é adotada somente em caso de pedido do titular dos dados. Isso reforça a ideia do consentimento *opt-out*, exaltado na Tabela 5.1. Os direitos de Anonimização e de Oposição à Tomada de Decisões Automatizadas foram apontados como inexistentes na CCPA [25], além de que por meio do framework analysis, não foi possível identificar o direito de Retenção Consistente com Finalidade.

5.2 Estrutura do Guia

O guia proposto, nomeado *5L2FGuide — 5 Laws, 2 Frameworks Guide —*, foi desenvolvido no formato de uma página web. O acesso é gratuito, pela plataforma `https://xdalle.github.io/5L2FGuide/index.html` e o código-fonte aberto disponível em `https://gi`

Tabela 5.5: Comparação das definições das direitos de proteção de dados.

Direitos	**LGPD**	**GDPR**	**ADPPA**	**Privacy Act**	**CCPA**
Coleta Minimizada	✓ Y/S [45]	✓ Y/D	✓ Y/S [46]	✓ Y/D	✓ Y/C
Confirmação da Existência do Tratamento	✓ Y/S [38]	✓ Y/S [38]	✕ N/A	✓ Y/D	✓ Y/S [25],[47]
Acesso aos Dados	✓ Y/S [38]	✓ Y/S [38]	✓ Y/O	✓ Y/D	✓ Y/S [25],[47]
Correção dos Dados	✓ Y/S [38]	✓ Y/S [38]	✓ Y/O	✓ Y/S [25],[50]	✓ Y/O
Anonimização	✓ Y/S [38]	✓ Y/C	✕ N/A	✓ Y/D	✕ N/A
Portabilidade dos Dados	✓ Y/S [38]	✓ Y/S [38]	✓ Y/S [46]	✕ N/A	✓ Y/S [25],[47]
Eliminação dos Dados	✓ Y/S [38]	✓ Y/S [38]	✓ Y/O	✕ N/A	✓ Y/S [25],[47]
Informação das Entidades Participantes	✓ Y/S [38]	✓ Y/O	✓ Y/O	✓ Y/D	✓ Y/O
Informação da Possibilidade de Não Consentir	✓ Y/S [38]	✓ Y/D	✓ Y/C	✕ N/A	✓ Y/O
Revogação do Consentimento	✓ Y/S [38]	✓ Y/D	✓ Y/O	✓ Y/S [25]	✓ Y/S [25]
Contestação	✓ Y/O	✓ Y/S [38]	✓ Y/O	✕ N/A	✓ Y/S [25]
Processamento Consistente com Finalidade	✓ Y/D	✓ Y/D	✓ Y/S [46]	✓ Y/D	✓ Y/O
Retenção Consistente com Finalidade	✓ Y/D	✓ Y/D	✓ Y/S [46]	✓ Y/D	✕ N/A
Oposição à Tomada de Decisões Automatizadas	✓ Y/O	✓ Y/S [38]	✕ N/A	✕ N/A	✕ N/A
Restrição do Processamento	✓ Y/C	✓ Y/S [38]	✕ N/A	✕ N/A	✓ Y/O

`thub.com/xDalle/5L2FGuide`. Além disso, o guia é composto pelas páginas navegáveis: *Introduction*, *Scope*, *Definitions*, *Principles*, *Rights*, *Challenges* e *About*.

A página *Introduction* apresenta a finalidade do guia, que é como os desenvolvedores e suas respectivas organizações podem garantir a conformidade (parcial ou total) com as legislações de privacidade, por meio dos frameworks Privacy by Design e ISO/IEC 29100. Para desenvolvedores que possuem pouco ou nenhum conhecimento acerca das leis, foi implementado um carrossel de informações, que é responsável por introduzir cada uma das legislações e os frameworks aos leitores. A página *About* segue o mesmo padrão estrutural, todavia há disponibilização das informações acerca do autor e da orientadora, bem como as referências utilizadas para elaboração do guia.

As páginas *Scope* e *Definitions* também compartilham de uma mesma estruturação. Nelas, há uma breve explicação do que seriam escopo e definições nas legislações, respectivamente, além de detalhar termos essenciais que são utilizados pelas diretrizes. A Figura 5.2 apresenta um exemplo das informações vistas pelo usuário na página referente ao escopo, em que ocorre a separação do tema geral, conforme elucidado na Tabela 5.1. O mesmo ocorre para a página de definições, todavia conforme Tabela 5.2.

A página *Challenges*, por sua vez, apresenta de maneira semelhante uma rápida introdução aos desafios organizacionais e suas técnicas de mitigação para garantir a conformidade com as leis de proteção de dados. Além disso, em sua estruturação há uma divisão a

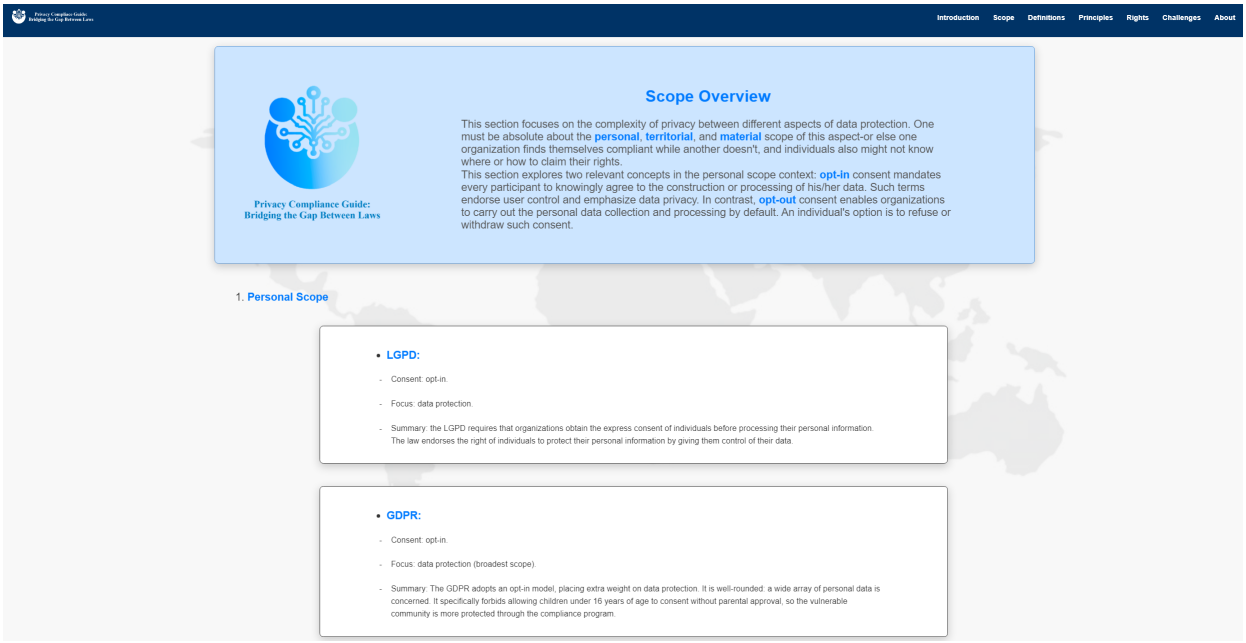


Figura 5.2: Página com informações comparativas explícitas ao leitor.

partir dos desafios identificados na RSL — Capítulo 3 — e, ademais, a inclusão dos novos desafios descobertos pelo survey, no capítulo seguinte. A Figura 5.3 reflete a visão inicial do leitor para essa página, bem como as divisões dos desafios enumerados.

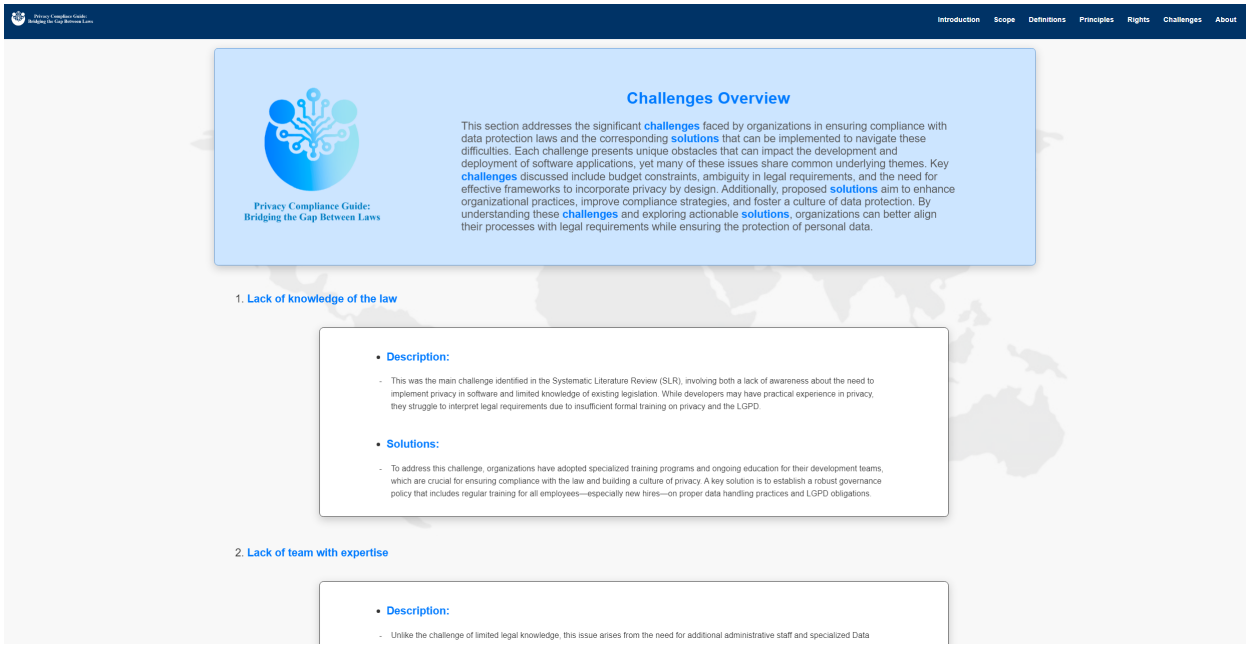


Figura 5.3: Página com informações acerca dos desafios e soluções da implementação das leis em software.

As páginas *Principles* e *Rights* são as páginas de maior carga teórica, haja vista Tabelas 5.4 e 5.5, logo a estruturação adotada para essas páginas foi diferente das demais. Uma vez

que o objetivo principal seria realizar uma comparação entre as leis e os frameworks, foi proposto um jogo interativo em que os usuários podem escolher inicialmente os princípios e os direitos que a organização precisa estar em conformidade. Como meio de facilitar essa seleção para desenvolvedores que conhecem apenas uma das leis ou um conjunto pequeno, é apresentado ao leitor a equivalência dos princípios e dos direitos explorada no framework analysis (Seção 5.1). A Figura 5.4 exemplifica o início do jogo na página *Principles*, em que o usuário deve escolher as cartas exigidas para conformidade em sua organização.

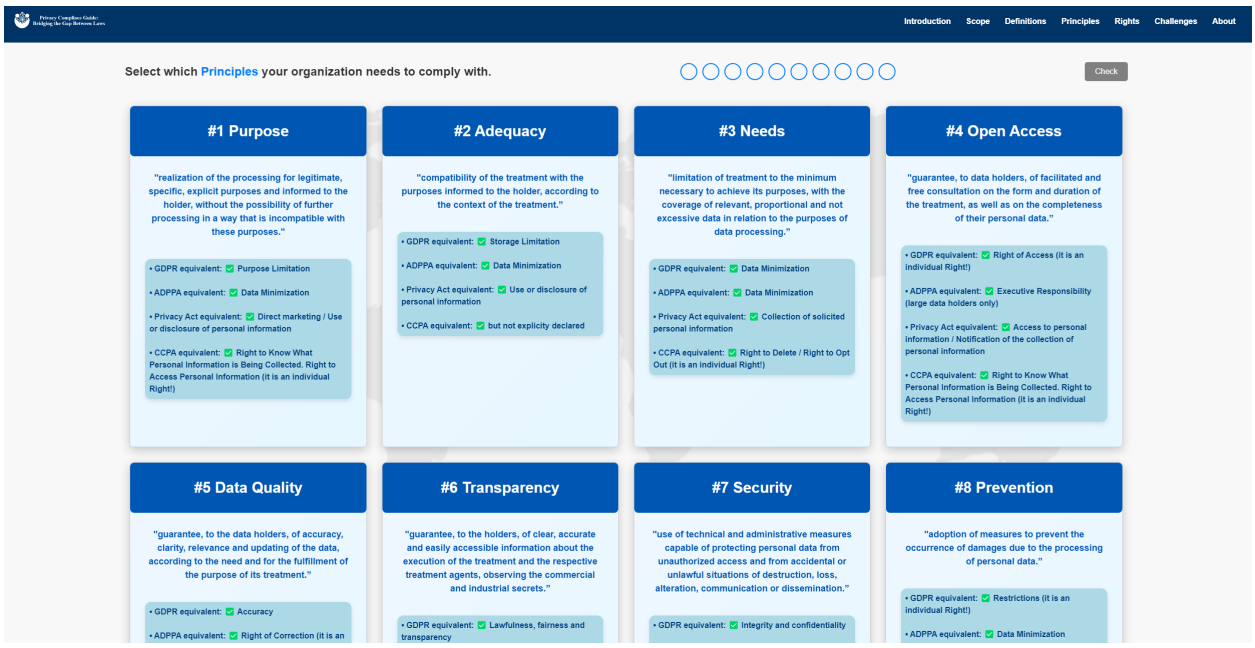


Figura 5.4: Página do jogo referente aos princípios.

No próximo passo, é apresentada a porcentagem de cobertura desses princípios e direitos por cada framework separadamente (e por ambos em conjunto), o que contribui para que o desenvolvedor escolha aquele que melhor atenda às demandas. A Figura 5.5 mostra as cartas selecionadas pelo usuário e os resultados referentes à cada framework. Vale lembrar que os frameworks também devem ser interpretados — por meio do processo de framework analysis — e, como podem ser mais superficiais do que as leis, o ideal é sempre utilizá-los como método de preencher lacunas, e não de substituição [24]. Os resultados apresentados buscam apenas informar como os princípios dos frameworks podem se relacionar com as leis estudadas.

Por fim, houve empenho para que todas as páginas pudessem introduzir um leitor, sem conhecimento prévio acerca das leis, de como interpretar as diretrizes e identificar os pontos em comum. Além disso, para desenvolvedores com alguma experiência em privacidade de dados, o guia focalizou em fornecer o conhecimento necessário para navegar de forma eficaz pelas regulamentações de privacidade e integrá-las nas práticas empresariais.

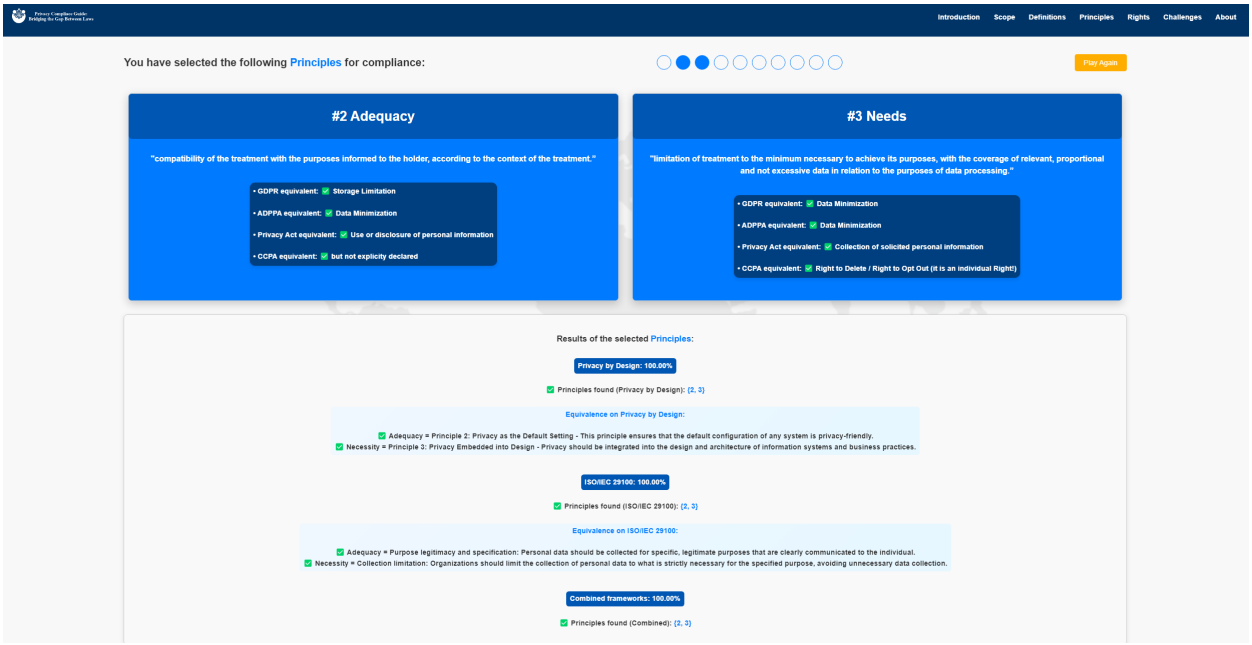


Figura 5.5: Página resultado do jogo referente aos princípios.

5.3 Desenvolvimento do Guia

5.3.1 Scope

Esta seção foca na complexidade da privacidade entre os diferentes aspectos da proteção de dados. É preciso ser absoluto no que diz respeito ao escopo pessoal, territorial e material deste aspecto – caso contrário, uma organização poderá estar em conformidade enquanto outra não está, e os indivíduos também poderão não saber onde ou como reivindicar os seus direitos.

Esta seção explora dois conceitos relevantes no contexto do escopo pessoal: o consentimento opt-in exige que cada participante concorde conscientemente com a coleta ou processamento de seus dados. Tais termos promovem o controle do usuário e enfatizam a privacidade dos dados. Por outro lado, o consentimento opt-out permite que as organizações realizem a coleta e o processamento de dados pessoais por padrão. A opção de um indivíduo é recusar ou retirar tal consentimento.

Personal Scope

- **LGPD:**
  - Consentimento: opt-in.
  - Foco: proteção de dados.

  - Resumo: a LGPD exige que as organizações obtenham o consentimento expresso dos indivíduos antes de processar suas informações pessoais. A lei exige o direito dos indivíduos de proteger suas informações pessoais, conferindo-lhes controle sobre seus dados.

- **GDPR:**
  - Consentimento: opt-in.
  - Foco: proteção de dados (escopo mais amplo).
  - Resumo: A GDPR adota um modelo opt-in, atribuindo maior importância à proteção de dados. É abrangente: uma ampla variedade de dados pessoais é considerada. Ele proíbe especificamente que crianças com menos de 16 anos consentam sem a aprovação dos pais, de modo que a comunidade vulnerável esteja mais protegida por meio do programa de conformidade.

- **ADPPA:**
  - Consentimento: opt-out.
  - Foco: liberdade corporativa.
  - Resumo: A ADPPA adota um modelo opt-out, ou seja, um sistema que permite o processamento de dados pessoais pelas organizações, a menos que os indivíduos optem por sair. Esse modelo favorece os interesses empresariais em detrimento dos direitos de privacidade individuais e, portanto, aumenta o temor de riscos em relação aos dados pessoais.

- **Australian Privacy Act:**
  - Consentimento: opt-in.
  - Foco: proteção de dados (escopo mais restrito).
  - Resumo: A Lei de Privacidade da Austrália adota uma abordagem opt-in, mas tem uma aplicação mais limitada na proteção de dados. Ela não reconhece uma diferença entre as obrigações dos controladores e processadores de dados, o que pode gerar ambiguidades na responsabilidade. Além disso, não restringe as crianças de fornecerem consentimento, expondo os menores a riscos.

- **CCPA:**
  - Consentimento: opt-out.
  - Foco: liberdade corporativa.

- Resumo: A CCPA utiliza um modelo opt-out, no qual os consumidores podem optar por não ter seus dados vendidos. Curiosamente, permite o consentimento de indivíduos maiores de 13 anos. De certa forma, isso permite que os menores tenham algum controle sobre seus dados pessoais.

Territorial Scope

- **LGPD:**
  - Aplica-se a organizações tanto dentro do Brasil quanto internacionalmente, desde que processem dados pessoais de residentes brasileiros. Esse enorme escopo de jurisdição garante que qualquer instituição interessada no processamento de dados pessoais de residentes brasileiros tenha que cumprir suas disposições, independentemente de onde a instituição esteja localizada.
- **GDPR:**
  - Aplica-se a qualquer organização dentro da UE, bem como àquelas fora da UE que processam dados pessoais de indivíduos residentes na UE. A aplicação jurisdicional cruzada destaca a necessidade de proteção no domínio dos dados em várias fronteiras.
- **ADPPA:**
  - Aplica-se diretamente às atividades de processamento de dados relacionadas a pessoas residentes nos Estados Unidos, tornando sua jurisdição um pouco mais localizada em relação à LGPD e ao GDPR.
- **Australian Privacy Act:**
  - Aplica-se a entidades APP (Princípios de Privacidade Australianos), que podem estar localizadas tanto dentro quanto fora da Austrália, desde que coletem ou manuseiem dados pessoais de residentes australianos.
- **CCPA:**
  - Aplica-se especificamente a empresas com fins lucrativos que operam na Califórnia e que tenham receitas anuais superiores a $25 milhões e que manuseiem dados pessoais. Esta lei estabelece um critério específico para a aplicabilidade, focando na escala das operações.

Material Scope

- **LGPD:**
  - Inclui dados pessoais sensíveis, que estão diretamente associados a indivíduos identificáveis. Isso se estende a qualquer dado que possa ser vinculado a uma pessoa, garantindo, assim, uma proteção abrangente das informações pessoais.
- **GDPR:**
  - Inclui dados pessoais sensíveis, que podem incluir associações diretas e indiretas. Notavelmente, inclui dados pessoais de funcionários, enfatizando a proteção de informações sensíveis em vários contextos, incluindo emprego.
- **ADPPA:**
  - Inclui dados pessoais sensíveis, mas não cobre especificamente os dados pessoais de funcionários, focando mais na proteção dos dados dos consumidores.
- **Australian Privacy Act:**
  - Inclui dados pessoais sensíveis, que são definidos de forma ampla para abranger vários tipos de informações pessoais. No entanto, não inclui especificamente os dados pessoais de funcionários, refletindo uma abordagem diferente em relação à privacidade no local de trabalho, mas considera de forma única opiniões como dados pessoais.
- **CCPA:**
  - Inclui dados pessoais sensíveis; no entanto, similar à ADPPA, não cobre explicitamente os dados pessoais de funcionários.

5.3.2 Definitions

Esta seção foca nos conceitos-chave que fornecem a base para as leis de proteção de dados em diferentes jurisdições. Cada lei tem suas peculiaridades; no entanto, a maioria utiliza nomenclaturas semelhantes ao se referir às disposições relacionadas ao processamento e à proteção de dados. Os termos incluídos são Dados Pessoais, Dados Sensíveis e os papéis dos controladores e processadores de dados. Dentro desse contexto, os termos são esclarecidos para ajudar o leitor a obter uma compreensão geral de como essas leis governam a proteção de dados e a privacidade.

Por exemplo, Dados Pessoais significam qualquer informação que identifique ou possa ser usada para identificar um indivíduo, enquanto Dados Sensíveis significam qualquer informação que necessite de proteção especial devido à sua natureza sensível.

Responsável pelo Processamento de Dados

- **LGPD:**
  - No contexto da LGPD, o controlador, o operador e o encarregado de proteção de dados (DPO) são as principais entidades responsáveis pelo tratamento de dados pessoais. O controlador determina a finalidade e os meios do tratamento de dados; o operador, em nome do controlador, processa os dados; e o encarregado de proteção de dados supervisiona as questões relacionadas às políticas de proteção de dados e atua como intermediário com a autoridade nacional de proteção de dados (ANPD).
- **GDPR:**
  - A GDPR identifica diferentes papéis envolvidos no tratamento de dados pessoais, incluindo o controlador (a entidade que determina as finalidades e os meios do tratamento de dados pessoais), o processador (a entidade que processa dados pessoais em nome do controlador) e o DPO que supervisiona a conformidade com as leis de proteção de dados e os processos para o tratamento seguro de dados pessoais dentro de uma organização.
- **ADPPA:**
  - No contexto da ADPPA, as entidades responsáveis pelo tratamento de dados são categorizadas como entidades cobertas e prestadores de serviços. Entidades cobertas referem-se a organizações ou empresas que coletam, processam ou transferem dados cobertos, que dizem respeito a indivíduos identificáveis, enquanto prestadores de serviços são entidades que processam dados em nome das entidades cobertas.
- **Australian Privacy Act:**
  - De acordo com a Lei de Privacidade da Austrália, as principais entidades responsáveis pelo tratamento de dados são conhecidas como Entidades APP (Entidades dos Princípios de Privacidade Australianos). Essas são as organizações ou agências que devem cumprir os Princípios de Privacidade Australianos (APPs) e geralmente incluem agências federais e certas outras organizações do

setor privado consideradas responsáveis pelo tratamento de dados pessoais em conformidade com as disposições da Lei.

- **CCPA:**
  - A Lei de Privacidade do Consumidor da Califórnia separa o controlador de dados do processador de dados. De acordo com a CCPA, as empresas são as entidades que coletam, usam ou divulgam as informações pessoais dos consumidores da Califórnia, enquanto o prestador de serviços é definido como uma entidade que processa essas informações em nome da empresa. Ambas devem cumprir as regulamentações da CCPA relacionadas à transparência sobre como lidam com os dados pessoais.

Dados Pessoais

- **LGPD:**
  - De acordo com a LGPD, dados pessoais referem-se a qualquer informação relacionada a uma pessoa identificada ou identificável. Definições tão amplas garantem que dados, desde os mais simples até os mais complexos, incluindo nomes, números de identificação, dados de localização, identificadores online ou fatores específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social de um indivíduo, estejam sob a proteção da lei.
- **GDPR:**
  - Os dados pessoais são aqueles que estão vinculados a pessoas naturais identificáveis de acordo com a GDPR. Isso pode incluir nome, número de identificação, dados de localização ou fatores específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa. A regulamentação diz respeito a qualquer informação que seja capaz de identificar alguém, direta ou indiretamente.
- **ADPPA:**
  - A ADPPA define dados cobertos como qualquer informação relacionada a uma pessoa natural identificada ou identificável. Esses dados cobertos abrangem uma categoria bastante ampla de informações que podem identificar direta ou indiretamente uma pessoa em particular; por exemplo, nomes, informações de contato ou identificadores online.
- **Australian Privacy Act:**

  - De acordo com a legislação australiana, dados pessoais representam qualquer informação que diz respeito a um indivíduo e é mantida por uma agência federal ou uma entidade APP. Esta é uma definição bastante ampla e certamente inclui informações que apontam ou provavelmente apontam direta ou indiretamente para um indivíduo, como nomes, detalhes de contato ou números de identificação, bem como opiniões ou inferências sobre o indivíduo.

- **CCPA:**

  - A CCPA define dados pessoais de forma ampla como qualquer informação que identifique, descreva ou possa ser associada a um consumidor ou sua família. Essa definição ampla inclui nomes, endereços, endereços de e-mail, informações sobre o histórico de navegação de um consumidor, registros de compras ou até mesmo inferências sobre as preferências ou comportamentos do consumidor. Um dos principais objetivos da CCPA é permitir que os consumidores tenham algum controle sobre suas informações pessoais, pois os informa sobre as informações coletadas, a finalidade para a qual são destinadas e como estão sendo utilizadas.

Dados Sensíveis

- **LGPD:**

  - Dados sensíveis são definidos sob a LGPD como um subconjunto de dados pessoais, especialmente aqueles que podem revelar origem racial ou étnica, crenças religiosas, opiniões políticas, filiação a sindicatos ou organizações religiosas, filosóficas ou políticas, vida sexual ou de saúde, dados genéticos ou biométricos. Essa proteção assegura privacidade e melhor dignidade em relação às ameaças em evolução.

- **GDPR:**

  - Dados sensíveis, ou categorias especiais de dados pessoais sob a GDPR, referem-se a tipos de informações mais delicadas que requerem proteção adicional. As informações relacionadas à origem racial ou étnica de uma pessoa, opiniões políticas, crenças religiosas ou filosóficas, filiação a um sindicato, dados genéticos, dados biométricos de um indivíduo, informações relacionadas à saúde ou à vida sexual ou orientação sexual de uma pessoa são classificadas como dados sensíveis.

- **ADPPA:**

  - Dados sensíveis sob a ADPPA foram designados como dados cobertos sensíveis, que são quaisquer informações pessoais que estão particularmente em risco de uso indevido ou que, se mal gerenciadas, podem resultar em danos significativos. Inclui informações como origem racial ou étnica, crenças religiosas, orientação sexual, informações biométricas e informações relacionadas à saúde. A ADPPA estabelece regulamentações mais rigorosas sobre dados cobertos sensíveis e, geralmente, requer o consentimento expresso do indivíduo afetado antes da sua coleta ou uso.

- **Australian Privacy Act:**

  - Dados sensíveis incluem quaisquer informações sobre um indivíduo que são mantidas por uma agência federal. Essas informações recebem uma proteção maior considerando sua natureza sensível; tais detalhes podem relacionar-se à origem racial ou étnica de uma pessoa, opiniões políticas, crenças religiosas, orientação sexual ou informações de saúde.

- **CCPA:**

  - Dados sensíveis sob a CCPA incluem informações que identificam, descrevem ou podem ser associadas a um consumidor ou sua família, de maneira semelhante aos dados pessoais. No entanto, é uma classe específica que abrange principalmente tipos de informações que, se divulgadas publicamente, criariam riscos muito sérios para a privacidade. Esses podem incluir tipos de dados sobre a geolocalização de um consumidor, raça/etnia, crenças religiosas ou políticas, saúde e dados financeiros, assim, a CCPA permite que os consumidores limitem o uso de informações sensíveis devido a diferentes direitos.

Processador de Dados

- **LGPD:**

  - Os processadores sob a LGPD são considerados quaisquer entidades que processam dados pessoais em nome do controlador, ou seja, o operador. Eles não determinam as finalidades da coleta de dados, mas permitem o manuseio seguro dos dados e a conformidade com a lei por parte da proteção de dados.

- **GDPR:**

  - Um processador sob a GDPR é uma entidade, seja uma pessoa natural ou jurídica, que processa dados pessoais em nome de um controlador. As obrigações

diretas impostas aos processadores incluem a manutenção de registros das atividades de processamento, e os processadores devem implementar medidas de segurança apropriadas.

- **ADPPA:**
  - Um processador de dados, sob a disposição da ADPPA, é definido como um prestador de serviços, ou seja, qualquer pessoa ou entidade jurídica que processa dados em nome de uma entidade coberta. Seu papel é ajudar as entidades cobertas na gestão de dados pessoais; no entanto, eles próprios devem adotar os parâmetros de segurança mais rigorosos para evitar qualquer acesso não autorizado ou violações.
- **Australian Privacy Act:**
  - Ao contrário de outras leis de privacidade, a Lei de Privacidade da Austrália não distingue especificamente entre controladores e processadores da mesma forma. O foco é principalmente em agências federais e entidades APP como controladores de dados pessoais, sem referência explícita a processadores de dados. Portanto, em situações regulares, a agência ou entidade que possui os dados será responsável pelo seu processamento, reduzindo assim a incidência de processadores de dados terceirizados oficiais.
- **CCPA:**
  - O processador de dados sob a CCPA é referido como prestador de serviços, que é qualquer entidade que processa informações pessoais em nome de uma empresa. Os prestadores de serviços estão vinculados por contratos com as empresas e são obrigados a conformar seu uso e divulgação de dados a diretrizes detalhadas. Isso significa que os prestadores de serviços não podem usar informações pessoais para seus próprios fins além do que está estipulado pela empresa que servem.

5.3.3 Principles

Esta seção apresenta os dez princípios da LGPD e como são comparados com as outras legislações. Um jogo interativo ilustra esses princípios, levando o usuário a escolher entre diferentes diretrizes (representadas como cartas), que mostram o grau de cobertura de uma diretriz específica de acordo com frameworks como a ISO/IEC 29100 e o Privacy by Design.

Assim, o usuário pode escolher os princípios para jogar e receber uma análise de cobertura sobre o quanto cada princípio atende aos requisitos legais. Dessa forma, os usuários têm uma experiência prática que permite visualizar onde e como os princípios de proteção de dados são aplicados na prática, dando uma visão de qual framework fornece a melhor base para cumprir os requisitos de conformidade. A Tabela 5.6 aponta como os princípios estão relacionados no guia.

Tabela 5.6: Mapeamento dos princípios e correlação entre leis.

LGPD	**GDPR**	**ADPPA**	**Privacy Act**	**CCPA**
Finalidade	✓ Purpose Limitation	✓ Data Minimization	✓ Direct marketing / Use or disclosure of personal information	✓ Right to Know What Personal Information is Being Collected. Right to Access Personal Information
Adequação	✓ Storage Limitation	✓ Data Minimization	✓ Use or disclosure of personal information	✓ but not explicity declared
Necessidade	✓ Data Minimization	✓ Data Minimization	✓ Collection of solicited personal information	✓ Right to Delete / Right to Opt Out
Livre Acesso	✓ Right of Access	✓ Executive Responsibility	✓ Access to personal information / Notification of the collection of personal information	✓ Right to Know What Personal Information is Being Collected. Right to Access Personal Information
Qualidade dos Dados	✓ Accuracy	✓ Right of Correction	✓ Quality of personal information / Correction of personal information	×
Transparência	✓ Lawfulness, fairness and transparency	✓ Right of Transparency	✓ Open and transparent management of personal information	✓ Right to Know What Personal Information is Being Collected. Right to Access Personal Information
Segurança	✓ Integrity and confidentiality	✓ Right of Data Security	✓ Security of personal information	✓ Security procedures and practices
Prevenção	✓ Restrictions	✓ Data Minimization	✓ Security of personal information	✓ Security procedures and practices
Não Discriminação	✓ Restrictions	✓ Data Minimization	×	✓ Right of No Retaliation
Responsabilização	✓ Accountability	✓ Executive Responsibility	×	✓ Right of No Retaliation

Em seguida, nos resultados, é apresentada a correlação entre os princípios base (LGPD) e os frameworks. A seleção segue o mesmo processo do framework analysis, focalizando

em termos específicos que apareçam em ambas diretrizes. A Tabela 5.7 elucida essa correlação.

Tabela 5.7: Mapeamento dos princípios da LGPD e correlação entre frameworks.

LGPD	**Privacy by Design**	**ISO/IEC 29100**
Finalidade	✕ [23]	✓ Consent and choice / Purpose legitimacy and specification [14], [23]
Adequação	✓ Privacy as the Default Setting [25]	✓ Collection limitation [14], [23]
Necessidade	✓ Proactive not Reactive; Preventive not Remedial / Privacy as Default Setting / Privacy Embedded into Design [25]	✓ Data minimization [14], [25]
Livre Acesso	✓ Visibility and Transparency [23], [25]	✓ Individual participation and access [14]
Qualidade dos Dados	✓ Proactive not Reactive; Preventive not Remedial [25]	✓ Accuracy and quality [14], [23], [25]
Transparência	✓ Visibility and Transparency [23], [25]	✓ Openness, transparency and notice [14], [23], [25]
Segurança	✓ End-to-End Protection [23]	✓ Information security [14], [23], [25]
Prevenção	✓ Proactive not Reactive; Preventative not Remedial	✓ Privacy compliance [14]
Não Discriminação	✓ Respect for User Privacy [25]	✕ [14]
Responsabilização	✕ [23]	✓ Accountability [14], [23], [25]

5.3.4 Rights

Esta seção foca de forma semelhante nos direitos essenciais estabelecidos por diversas leis de proteção de dados. Assim como na seção 5.3.3, é implementado um jogo interativo que permite os usuários explorar esses direitos e ver como a ISO/IEC 29100 e o Privacy by Design se alinham a eles.

Por meio dessa abordagem, o intuito é o mesmo: oferecer uma visão prática da cobertura dos direitos, ajudando os usuários a compreender o nível de proteção oferecido por cada framework. A Tabela 5.8 mostra a relação dos direitos garantidos pela LGPD — nem todos especificados em seção específica — e das demais legislações.

Acerca dos resultados, é proposta a correlação entre os direitos garantidos pela LGPD e os frameworks. Assim como foi feito para os princípios, é adotado o processo do framework analysis, identificando termos específicos que apareçam em ambas diretrizes. A Tabela 5.9 apresenta essa correlação.

5.3.5 Challenges

Esta seção aborda os desafios significativos enfrentados pelas organizações na garantia da conformidade com as leis de proteção de dados e as soluções correspondentes que podem

Tabela 5.8: Mapeamento dos direitos e correlação entre leis.

LGPD	**GDPR**	**ADPPA**	**Privacy Act**	**CCPA**
Coleta Minimizada	✓ Data Minimization	✓ Data Minimization	✓ Collection of solicited personal information	✓ Right to Limit Use and Disclosure of Sensitive Personal Information
Confirmação da Existência do Tratamento	✓ Right of access by the data subject	×	✓ Access to personal data	✓ Right to Know What Personal Information is Being Collected. Right to Access Personal Information
Acesso aos Dados	✓ Right of access by the data subject	Right to Access	✓ Right to Access	✓ Right to Know What Personal Information is Being Collected. Right to Access Personal Information
Correção dos Dados	✓ Right to rectification	✓ Right to Correct	✓ Right to Correct	✓ Right to Correct Inaccurate Personal Information
Anonimização	✓ Pseudonymisation	×	✓ Anonymity and pseudonymity	×
Portabilidade dos Dados	✓ Right to data portability	✓ Right to Portability	×	✓ Right to Know What Personal Information is Being Collected. Right to Access Personal Information
Eliminação dos Dados	✓ Right to erasure	✓ Right to Delete	×	✓ Right to Delete Personal Information
Informação das Entidades Participantes	✓ Information to be provided where personal data are collected from the data subject	✓ Right of Transparency	✓ Open and transparent management of personal information	✓ Right to Know What Personal Information is Sold or Shared and to Whom
Informação da Possibilidade de Não Consentir	✓ Right to withdraw	✓ Right of Transparency	×	✓ Right to Opt Out of Sale or Sharing of Personal Information
Revogação do Consentimento	✓ Right to withdraw	✓ Right to Consent and Object	✓ Collection of solicited personal information / Use or disclosure of personal information	✓ Right to Opt Out of Sale or Sharing of Personal Information
Contestação	✓ Right to contest / Right to lodge a complaint with a supervisory authority	✓ Right to Consent and Object	×	✓ Right to Opt Out of Sale or Sharing of Personal Information
Processamento Consistente com Finalidade	✓ Storage limitation	✓ Data Minimization	✓ Use or disclosure of personal information	✓ Right to Know What Personal Information is Being Collected. Right to Access Personal Information
Retenção Consistente com Finalidade	✓ Storage limitation	✓ Data Retention policies	✓ Security of personal information	×
Oposição à Tomada de Decisões Automatizadas	✓ Automated individual decision-making, including profiling	×	×	×
Restrição do Processamento	✓ Right to restriction of processing	×	×	✓ Right to Limit Use and Disclosure of Sensitive Personal Information

Tabela 5.9: Mapeamento dos direitos da LGPD e correlação entre frameworks.

LGPD	**Privacy by Design**	**ISO/IEC 29100**
Coleta Minimizada	✓ Proactive not Reactive; Preventative not Remedial / Privacy as the Default Setting / Privacy Embedded into Design [25]	✓ Data minimization [23]
Confirmação da Existência do Tratamento	✓ Visibility and Transparency [25]	✓ Openness, transparency and notice [25]
Acesso aos Dados	✓ Visibility and Transparency [25]	✓ Individual participation and access [25]
Correção dos Dados	✕ [23]	✓ Individual participation and access [25]
Anonimização	✕ [23]	✓ Use, retention and disclosure limitation [23]
Portabilidade dos Dados	✓ Respect for User Privacy [25]	✓ Use, retention and disclosure limitation [23]
Eliminação dos Dados	✕ [23]	✓ Individual participation and access
Informação das Entidades Participantes	✓ Visibility and Transparency [25]	✓ Openness, transparency and notice [25]
Informação da Possibilidade de Não Consentir	✓ Visibility and Transparency [25]	✓ Consent and choice [25]
Revogação do Consentimento	✓ Proactive not Reactive; Preventative not Remedial / Respect for User Privacy [25]	✓ Consent and choice [25]
Contestação	✓ Respect for User Privacy [25]	✓ Accountability [25]
Processamento Consistente com Finalidade	✓ Privacy as The Default Setting [25]	✓ Collection limitation [14], [25]
Retenção Consistente com Finalidade	✓ Respect for User Privacy [23], [25]	✓ Use, retention and disclosure limitation
Oposição à Tomada de Decisões Automatizadas	✓ Respect for User Privacy [25]	✕ [25]
Restrição do Processamento	✓ Proactive not Reactive; Preventative not Remedial [25]	✕ [25]

ser implementadas para lidar com essas dificuldades. Cada desafio apresenta obstáculos únicos que podem impactar o desenvolvimento e a implementação de aplicativos de software, mas muitos desses problemas compartilham temas subjacentes comuns.

Os principais desafios discutidos incluem restrições orçamentárias, ambiguidade nos requisitos legais e a necessidade de estruturas eficazes para incorporar a privacidade desde a concepção. Além disso, as soluções propostas visam aprimorar as práticas organizacionais, melhorar as estratégias de conformidade e promover uma cultura de proteção de dados. Ao entender esses desafios e explorar soluções acionáveis, as organizações podem alinhar melhor seus processos aos requisitos legais, garantindo a proteção dos dados pessoais.

Escassez de conhecimento da lei

- **Descrição**
  - Esse foi o principal desafio identificado na Revisão Sistemática da Literatura (SLR), envolvendo tanto a falta de conscientização sobre a necessidade de implementar a privacidade no software quanto o conhecimento limitado da legislação existente. Embora os desenvolvedores possam ter experiência prática em privacidade, eles têm dificuldades para interpretar os requisitos legais devido à insuficiência de treinamento formal sobre privacidade e a LGPD.
- **Soluções**
  - Para enfrentar esse desafio, as organizações adotaram programas de treinamento especializados e educação contínua para suas equipes de desenvolvimento, que são cruciais para garantir a conformidade com a lei e construir uma cultura de privacidade. Uma solução chave é estabelecer uma política de governança robusta que inclua treinamento regular para todos os funcionários — especialmente novos contratados — sobre práticas adequadas de manuseio de dados e obrigações da LGPD.

Traduzir a lei para um contexto técnico

- **Descrição**
  - Os desenvolvedores enfrentam desafios ao interpretar normas teóricas de privacidade que carecem de técnicas específicas de conformidade. Essa complexidade torna difícil traduzir os requisitos legais em práticas organizacionais, deixando muitos desenvolvedores desconfortáveis. Eles também têm dificuldades com a

anonimização de dados e processos de automação. Estruturas como Privacidade por Design e Privacidade por Default são recomendadas.

- **Soluções**
  - Os desenvolvedores sugeriram o uso de uma Política de Classificação de Informações para catalogar e rotular dados, com ferramentas de código aberto como Openmetadata e Datahub para assistência. É essencial estabelecer estratégias de proteção, incluindo medidas criptográficas e descarte de dados, conforme exigido pela LGPD.

Restrições de orçamento

- **Descrição**
  - Esse é um obstáculo comum que afeta principalmente as organizações, com os desenvolvedores tendo pouca ou nenhuma influência sobre ele. Aproximadamente um ano após a entrada em vigor da GDPR, estudos mostraram que a conformidade com a lei é cara e demorada, exigindo recursos financeiros e humanos contínuos que as organizações muitas vezes têm em quantidade limitada. Há uma associação direta entre operações de segurança e um aumento nos orçamentos organizacionais; assim, o nível de privacidade e segurança dos dados está intimamente ligado ao capital disponível. Esse desafio é particularmente crítico para pequenas e médias empresas.
- **Soluções**
  - Uma solução proposta é adotar um design de privacidade proativo, contrastando com soluções que vinculam as normas da GDPR aos requisitos comerciais. Alguns desenvolvedores sugeriram utilizar ferramentas de código aberto, especialmente aquelas que são populares e robustas em ambientes profissionais. Essa abordagem permite que as organizações abordem questões imediatas relacionadas à conformidade com a LGPD, mesmo que não possam alocar atualmente capital significativo para essa área.

Falta equipe com expertise

- **Descrição**
  - Diferentemente do desafio do conhecimento legal limitado, esse problema surge da necessidade de mais pessoal administrativo e de Encarregados pela Proteção

de Dados (DPOs) especializados. Sem uma equipe capacitada, as avaliações de risco para a proteção de dados podem ser ineficazes e a conformidade com a LGPD brasileira pode estar incompleta.

- **Soluções**
  - Uma solução simples é nomear um DPO ou contratar consultores especializados ou equipes jurídicas para validação de conformidade. No entanto, os desenvolvedores também sugeriram treinamento contínuo e conscientização para a equipe existente que lida com dados para abordar as lacunas de expertise. Outra sugestão inovadora envolve o uso de Processamento de Linguagem Natural para detectar automaticamente dados sensíveis durante o processamento, alertando as partes responsáveis sobre possíveis problemas de conformidade sem exigir conhecimento legal prévio.

Estrutura organizacional

- **Descrição**
  - Frequentemente, há uma lacuna de comunicação entre especialistas em privacidade e desenvolvedores de software, o que dificulta a implementação adequada da privacidade nas aplicações devido à ausência de códigos de conduta necessários. As organizações podem impor limitações aos funcionários, resultando em não conformidade regulatória. A gestão eficaz do conhecimento é crucial para a organização interna e conformidade com a legislação.
- **Soluções**
  - Projetos de comunicação estratégica, como planos de sistemas de informação ou Programas Institucionais de Privacidade de Dados, podem ajudar a melhorar a cultura organizacional. Além disso, uma governança adequada e acesso limitado a dados sensíveis são importantes. A implementação de segurança em nível de linha (RLS) pode ajudar a determinar quais informações compartilhar, e arquiteturas como a Arquitetura Medallion da Microsoft podem facilitar a interação entre desenvolvedores e especialistas em privacidade. Além disso, o uso de dados fictícios e a restrição do acesso a bancos de dados de produção podem garantir a conformidade com a LGPD, mesmo entre filiais.

Ambiguidade da lei

- **Descrição**

  - Muitos desenvolvedores lutam para cumprir as regulamentações quando são vagas, complicando a extração e a implementação dos requisitos legais. Quando os requisitos não são expressos em uma linguagem clara e específica, podem ser interpretados de várias maneiras, levando a um nível de privacidade que pode não estar alinhado com a intenção legislativa.

- **Soluções**

  - Mapear as leis de privacidade para estruturas de privacidade desde o início e utilizar padrões de design, como chaves de criptografia gerenciadas pelo usuário e adição de ruído para ofuscação de dados. Uma solução prática imediata é empregar uma estratégia de prevenção para quaisquer conjuntos de dados, enfatizando a minimização de dados — coletando apenas os dados necessários para atingir os objetivos de tratamento — e mascarando e criptografando todos os dados como métodos eficazes para mitigar danos em caso de violação.

Falta padronização de técnicas/ferramentas

- **Descrição**

  - Há uma falta de padronização e métricas de avaliação para práticas de privacidade, uma vez que o conceito de privacidade é volátil e varia de projeto para projeto. Embora existam taxonomias e estruturas para implementar a privacidade, não há consenso sobre elas, e a legislação existente carece de diretrizes específicas sobre quais tecnologias utilizar. Consequentemente, as organizações devem encontrar soluções personalizadas para a conformidade. Esse desafio é agravado pela ausência de técnicas, ferramentas ou metodologias padronizadas para garantir a conformidade legal.

- **Soluções**

  - Possíveis soluções incluem aderir às diretrizes da plataforma de publicação do aplicativo e utilizar várias tecnologias, como controle de acesso, criptografia SHA256, anonimização, VPNs privadas e gerenciamento transparente de consentimento. A comunicação regular entre os membros da equipe, semelhante às metodologias ágeis como o Scrum, é crucial para manter todos informados sobre as tecnologias recomendadas e seus detalhes.

Falta política de segurança/privacidade

- **Descrição**

  - A criação de um formulário de consentimento e uma política de segurança continua sendo um desafio frequentemente negligenciado pelas organizações. Muitas empresas carecem de medidas de segurança documentadas e não possuem procedimentos para notificar as autoridades em caso de violações de dados pessoais. Esse problema pode se originar dos desenvolvedores também, especialmente quando usam bibliotecas de terceiros, o que pode dificultar sua compreensão das aplicações e impedir o desenvolvimento adequado de uma política de privacidade.

- **Soluções**

  - Redação transparente de termos de uso, a revisão das bases legais para criar uma política de segurança eficaz e atualizada, e a utilização de técnicas como rastreamento de terceiros e configurações de API. Os desenvolvedores destacaram três pontos-chave para garantir a segurança dos dados: criptografia de banco de dados, anonimização quando necessário (e evitando dados sensíveis sempre que possível) e controle de acesso com gerenciamento de permissões. Com um mapeamento minucioso dos dados coletados, as organizações podem revisar as políticas internas e avaliar riscos e respostas a incidentes para garantir que sua política de segurança seja robusta e esteja em conformidade com a LGPD.

Relacionamento com o usuário

- **Descrição**

  - As regulamentações de privacidade atuais concedem aos usuários vários direitos — como portabilidade de dados, correção e exclusão — que influenciam ativamente como seus dados pessoais são processados. Estudos identificaram desafios na relação entre usuários e organizações ou desenvolvedores, particularmente em relação ao processo de consentimento, já que alguns usuários podem ser indiferentes aos benefícios da privacidade. Os desenvolvedores também enfrentam dificuldades em implementar transparência por meio de políticas de privacidade e sistemas de solicitação, complicando ainda mais a situação.

- **Soluções**

  - No entanto, empresas líderes como Microsoft e Google abordaram essas questões ao fornecer ferramentas de autoatendimento e painéis de privacidade.

Além disso, é benéfico envolver os usuários em todo o processamento de dados, garantindo que eles estejam cientes e consentindo com todo o processo, especialmente em testes de usabilidade que exigem gravação.

Priorização de requisitos funcionais

- **Descrição**
  - Os desenvolvedores enfrentam desafios em priorizar requisitos funcionais, muitas vezes devido a fatores como a redução do desempenho do sistema, prazos apertados para a implementação eficaz da segurança e as dificuldades inerentes aos requisitos não funcionais. Existe uma tensão entre priorizar requisitos funcionais e garantir segurança e privacidade, complicando a conformidade com a legislação de privacidade.
- **Soluções**
  - Para enfrentar a pressão dos prazos, testes automatizados podem aprimorar o foco nos requisitos não funcionais, enquanto métodos que facilitam atualizações rápidas do aplicativo e feedback eficaz podem motivar os desenvolvedores a melhorar ambas as categorias. Muitos desenvolvedores enfatizam a consideração dos requisitos de privacidade desde o início do projeto, utilizando técnicas como a estrutura de Privacidade por Design, criando componentes arquitetônicos reutilizáveis, implementando práticas de baixo custo como criptografia SHA256, utilizando ferramentas de população de bancos de dados para testes e mapeando continuamente dados pessoais. Essa abordagem garante que a privacidade seja mantida ao longo do desenvolvimento.

Incerteza dos processos organizacionais

- **Descrição**
  - Os desenvolvedores podem não estar sempre familiarizados com todos os processos organizacionais, o que complica a conformidade com a legislação de proteção de dados. Isso leva a desafios na adequação de backup de dados, auditorias de sistemas e uso de serviços em nuvem, que dependem da localização física do armazenamento de dados.
- **Soluções**
  - Para mitigar esses riscos, as organizações devem implementar registros de acesso para o processamento de dados e escolher provedores de nuvem que

garantam conformidade com as leis relevantes. Estabelecer uma governança de dados forte com controles de acesso claros é crucial. Centralizar dados em uma única aplicação, em vez de usar sistemas departamentais, e manter registros detalhados das operações de manuseio de dados pode reduzir a incerteza. Além disso, minimizar a coleta e a retenção de dados ajuda os desenvolvedores a entender como e quais dados são utilizados no sistema.

Dificuldades em serviços de terceiros

- **Descrição**
  - Muitas questões de privacidade surgem do uso de Kits de Desenvolvimento de Software (SDKs) de terceiros. Embora um aplicativo possa inicialmente estar em conformidade com a legislação de privacidade, a incorporação de SDKs não garante a conformidade contínua, uma vez que muitas empresas não examinam adequadamente esses contratos. Os desenvolvedores enfrentam dificuldades para navegar pelas implicações de privacidade dessas bibliotecas e entender como elas lidam com dados pessoais.
- **Soluções**
  - Priorizar bibliotecas de fornecedores respeitáveis e minimizar o compartilhamento de dados com terceiros apenas ao que é absolutamente necessário. É crucial garantir que todos os fornecedores e parceiros estejam em conformidade com as regulamentações de proteção de dados e evitar a transmissão de informações sensíveis que não são essenciais para o processamento. Além disso, o mapeamento minucioso do software e dos dados — incluindo documentação, informações do sistema e códigos de terceiros — é vital para que os desenvolvedores compreendam o uso e o armazenamento dos dados. Medidas de segurança de dados, como criptografia durante o armazenamento, transmissão e uso, também são essenciais para mitigar os riscos associados ao compartilhamento de informações. Por fim, estabelecer protocolos internos para verificar a integridade e a confiabilidade de bibliotecas e softwares de terceiros pode ajudar ainda mais a prevenir violações.

Escassez de guias/ferramentas

- **Descrição**
  - A ambiguidade na legislação de privacidade e os desafios na tradução dessas leis para um contexto técnico destacam a necessidade de guias e ferramentas

para auxiliar na conformidade. No entanto, os desenvolvedores no Brasil e na Europa relataram a falta de diretrizes específicas para aplicar a privacidade em contextos de software. Muitos desenvolvedores têm dificuldade em encontrar diretrizes de design apropriadas e, quando o fazem, o suporte é frequentemente inadequado para empresas menores.

- **Soluções**
  - Focar na experiência do usuário e consultar profissionais na ausência de recursos dedicados. Além disso, auditorias especializadas, interações com Encarregados pela Proteção de Dados (DPOs) e acesso a materiais informativos sobre a LGPD (Lei Geral de Proteção de Dados) são cruciais para compensar a falta de diretrizes direcionadas. Os desenvolvedores expressaram que ter fácil acesso a recursos informativos sobre a LGPD, incluindo normas e técnicas, é benéfico para toda a equipe. Eles também sugeriram que tutoriais em vídeo e folhetos proporcionariam um suporte significativo, facilitando o acesso à informação, especialmente uma vez que questões relacionadas à LGPD são tratadas principalmente pelas equipes de conformidade, em vez da equipe de desenvolvimento.

Processamento de dados internacionais

- **Descrição**
  - Esse foi um importante desafio identificado na Revisão Sistemática da Literatura (SLR), envolvendo tanto a falta de conscientização sobre a necessidade de implementar privacidade em software quanto o conhecimento limitado da legislação existente. Embora os desenvolvedores possam ter experiência prática em privacidade, eles lutam para interpretar os requisitos legais devido à falta de treinamento formal sobre privacidade e a LGPD.
- **Soluções**
  - Para abordar esse desafio, as organizações adotaram programas de treinamento especializados e educação contínua para suas equipes de desenvolvimento, que são cruciais para garantir a conformidade com a lei e construir uma cultura de privacidade. Uma solução-chave é estabelecer uma política de governança robusta que inclua treinamento regular para todos os funcionários — especialmente novos contratados — sobre as práticas adequadas de manuseio de dados e as obrigações da LGPD.

Mudanças nos estágios de desenvolvimento

- **Descrição**
  - Mudanças durante o processo de desenvolvimento do produto são comuns, variando desde o crescimento da infraestrutura e a expansão dos dados até ajustes destinados a melhorar a compatibilidade. Embora essas mudanças possam ser necessárias, elas aumentam a complexidade técnica e exigem revisões das técnicas que implementam privacidade no software. Equilibrar a conformidade com a GDPR em um ambiente competitivo de negócios de dados é um desafio notado.
- **Soluções**
  - Uma solução proposta é o uso de engenharia de software contínua, que permite atualizações rápidas e feedback, possibilitando correções rápidas de problemas de não conformidade identificados por meio de feedback. Portanto, quaisquer modificações no software necessitam de monitoramento adequado das leis aplicáveis e avaliações de impacto regulares. Essas avaliações permitem ajustes contínuos à medida que o software evolui. Além disso, alguns desenvolvedores indicaram que contratar consultores jurídicos especializados poderia ajudar a detectar não conformidades súbitas.

Trade-off ética X economia

- **Descrição**
  - As organizações frequentemente enfrentam o desafio de equilibrar o respeito à privacidade com a priorização da liberdade corporativa. Uma vez que o principal objetivo de uma empresa é econômico, a privacidade e a proteção de dados pessoais podem ser menosprezadas, mesmo na presença de leis de conformidade.
- **Soluções**
  - As organizações precisam considerar as potenciais penalidades administrativas por não conformidade, assim como a desvantagem competitiva de longo prazo e a perda de confiança dos clientes, que podem levar a perdas financeiras. É crucial apresentar claramente o uso pretendido dos dados em termos de consentimento e desvincular indivíduos de seus dados sempre que possível por meio da anonimização. Finalmente, os indivíduos devem ter o direito de acessar, modificar e excluir permanentemente suas informações mediante solicitação.

Identificação de requisitos de privacidade

- **Descrição**
  - Os desenvolvedores possuem conhecimento empírico sobre privacidade, mas identificar requisitos de privacidade em relação à legislação de proteção de dados é complexo. Uma avaliação ineficaz desses requisitos leva a problemas tanto na coleta de dados — selecionando dados desnecessários para o software, o que viola o princípio da necessidade — quanto no desenvolvimento, resultando em falhas de segurança que podem acarretar penalidades administrativas.
- **Soluções**
  - Para auxiliar na conformidade, é necessário utilizar ferramentas como especificações de histórias de usuários para facilitar a fase de análise de requisitos. Em equipes ágeis, empregar ferramentas de Design Thinking durante a fase de elicitação de requisitos também pode ser benéfico. O mapeamento do ciclo de vida dos dados (Inventário de Dados) ajuda a identificar e documentar todos os dados pessoais e seus fluxos, permitindo uma análise mais profunda do que é essencial para os propósitos do software e o que pode ser descartado. Além disso, a equipe de conformidade desempenha um papel crucial na mitigação desse desafio, particularmente quando os desenvolvedores enfrentam dificuldades com os aspectos teóricos da lei.

Impacto na usabilidade da aplicação

- **Descrição**
  - Essa questão é particularmente relevante para pequenas e médias empresas. Se as capacidades de processamento de dados forem insuficientes, a implementação de estruturas de privacidade e proteção de dados pode diminuir o desempenho do sistema ou prejudicar a usabilidade do aplicativo.
- **Soluções**
  - É aconselhável empregar estruturas específicas o mais cedo possível, durante o processo de design da aplicação, para estimar e mitigar riscos de desempenho. Uma técnica-chave de mitigação é a minimização de dados, que melhora a transparência dos termos de consentimento e reduz os impactos negativos potenciais na experiência do usuário. Consequentemente, organizar, processar e limpar dados se torna mais fácil, uma vez que as informações armazenadas

estão alinhadas com o princípio da necessidade definido nas regulamentações de privacidade.

Processo de desenvolvimento não avaliado institucionalmente à luz da LGPD

- **Descrição**
  - É comum que as organizações não tenham uma cultura focada na conformidade com a LGPD. Um dos principais desafios é a necessidade de modificar a arquitetura de software que já está em produção e que não foi projetada com os requisitos da LGPD em mente.
- **Soluções**
  - Para mitigar esse problema, recomenda-se usar estruturas estabelecidas ou criar um novo padrão que assegure a implementação da LGPD desde o início de cada projeto. Além disso, sugerem-se guias para mapear os requisitos da LGPD, alinhando esses requisitos com soluções dentro do processo de desenvolvimento.

Projetos criados sem privacidade por padrão

- **Descrição**
  - Essa questão é semelhante aos desafios associados a mudanças nas fases de desenvolvimento, mas está especificamente relacionada à falta de consideração pela privacidade durante a fase inicial. Falhas que violam a LGPD são frequentemente identificadas cedo no desenvolvimento e podem ser facilmente abordadas; no entanto, a prevenção é sempre preferível.
- **Soluções**
  - Portanto, recomenda-se definir as configurações de privacidade mais restritivas como padrões, exigindo nenhuma intervenção do usuário. Um desenvolvedor sugeriu o uso da estrutura Privacy by Design, uma vez que a privacidade por padrão é um de seus princípios fundamentais. Integrar a privacidade desde o início do desenvolvimento ajuda a garantir que ela seja um princípio central do projeto, prevenindo penalidades indesejadas e reduzindo a necessidade de retrabalho.

Constantes mudanças da lei

- **Descrição**

  - Dada a exigência de cumprir várias regulamentações complexas, o mapeamento e o acesso aos dados coletados devem ser ainda mais rigorosos, e a documentação do software deve incluir todas as mudanças, mesmo as recentes.

- **Soluções**

  - Para abordar essa questão, recomenda-se que a organização tenha um Plano de Resposta a Incidentes (IRP) eficaz em vigor para minimizar danos potenciais de quaisquer mudanças legislativas que ainda não foram implementadas no software. Além disso, é crucial que o software seja continuamente atualizado, com documentação de projeto atualizada, potencialmente vinculada a um processo de controle de versão.

5.4 Síntese deste Capítulo

Este capítulo apresentou o processo de análise de frameworks utilizado na etapa comparativa das legislações para o desenvolvimento do guia *5L2FGuide*, além da estrutura do guia em si. A estrutura e navegação da página web foram projetadas para oferecer uma experiência acessível e intuitiva, permitindo ao usuário explorar facilmente os tópicos de conformidade em proteção de dados. Em seguida, são apresentadas as informações contidas no guia — escopo, definições, princípios, direitos e desafios —, abrangendo a etapa de desenvolvimento e o conteúdo central, como os conceitos-chave e práticas recomendadas.

Capítulo 6

Validação da Ferramenta

Neste capítulo está detalhado o questionário aplicado para a validação do guia. O processo de validação explora a facilidade de uso e a utilidade do guia e são apresentadas a configuração, a elaboração e os resultados do survey, bem como as melhores implementadas no guia.

6.1 Configuração do Survey

O survey foi desenvolvido por meio da plataforma Google Forms, com tempo estipulado de 15 minutos, para a leitura integral do guia e o devido preenchimento das respostas. O guia foi apresentado para duas turmas de pós-graduação em Privacidade e Segurança da Informação, durante a disciplina de Gestão de Privacidade e Proteção de Dados Pessoais. Em seguida, foi solicitado que os participantes explorassem as seções do guia, desde os comparativos até os jogos, para posterior preenchimento do questionário.

Os participantes foram informados de que a participação é anônima, voluntária e exclusivamente para fins de pesquisa, sendo necessário o consentimento para participar. Além disso, foi explicado que o processo poderia ser interrompido a qualquer momento, sem penalidades ou registro parcial das respostas. Por fim, após a apresentação do trabalho, o autor se disponibilizou para sanar eventuais dúvidas quando do preenchimento do survey ou da interação com o guia.

6.2 Elaboração do Survey

Assim como o questionário elaborado no Capítulo 4, este se divide em duas partes: dados demográficos do participante e a validação do guia em si. Na Tabela 6.1 é possível visualizar as perguntas referentes ao perfil do participante e na Tabela 6.2 os questionamento

com o intuito de auxiliar na validação. Além disso, uma cópia do questionário pode ser visualizada na plataforma Zenodo [66], além das respostas coletadas.

Tabela 6.1: Perguntas relativas ao perfil do participante.

ID	Pergunta	Escala de resposta
Q01	Qual seu Estado?	Acre; Alagoas; Amapá; Amazonas; Bahia; Ceará; Distrito Federal; Espírito Santo; Goiás; Maranhão; Mato Grosso; Mato Grosso do Sul; Minas Gerais; Pará; Paraíba; Paraná; Pernambuco; Piauí; Rio de Janeiro; Rio Grande do Norte; Rio Grande do Sul; Rondônia; Roraima; Santa Catarina; São Paulo; Sergipe; Tocantins.
Q02	Qual é seu nível de escolaridade?	Estudante de graduação; graduado; especialização; estudante de mestrado; mestrado; estudante de doutorado; doutorado.
Q03	Qual é a sua função atual no seu trabalho?	Desenvolvedor de software; engenheiro de software; analista de requisitos; analista de sistemas; gerente de projeto; gestor de segurança da informação; encarregado de dados; operador de dados; controlador de dados; analista de segurança da informação; outro.
Q04	Quantos anos de experiência você tem na área de Privacidade de Dados?	Menos de 1 ano; entre 1 e 5 anos; entre 6 e 10 anos; entre 11 e 15 anos; mais de 15 anos.
Q05	Qual é a natureza da organização em que você trabalha?	Empresa privada; Agência da Administração Pública Federal; Projeto de pesquisa/colaboração; Empresa estatal (BB, CEF, SERPRO, DATAPREV); Projeto de software de código aberto; Autônomo; outro.
Q06	Você já pesquisou ou trabalho com leis de proteção de dados?	Sim; não.
Q07	Atualmente, você pesquisa ou trabalha com leis de proteção de dados?	Sim; não.
Q08	Qual seu nível de experiência ou conhecimento sobre leis de proteção de dados?	Nenhum; básico; intermediário; avançado.

De Q01 até Q05, estão incluídas as perguntas gerais acerca do perfil do participante, que tem o intuito de identificar e setorizar a amostra e, em seguida (Q06 até Q08), os respondentes informam sua experiência teórica e prática acerca de leis de proteção de dados.

Acerca das perguntas Q09 até Q17, os respondentes são apresentados com perguntas fundamentadas no Modelo de Aceitação de Tecnologia — *Technology Acceptance Model* (TAM) [100] —, com o intuito de medir dois fatores: o quanto o guia ajudaria o usuário em aprimorar seu trabalho (usabilidade) e se o guia não envolve um esforço excessivo para ser utilizado (facilidade de uso). Sendo assim, as perguntas de Q09 até Q13 buscam medir a usabilidade, enquanto Q14 até Q17 a facilidade de uso. Dessa forma, o respondente deve selecionar a alternativa em escala Likert do quanto concorda com cada afirmação.

Por fim, as perguntas Q18 até Q20 exigem resposta livre, isto é, o participante deve expressar com suas próprias palavras quais são os pontos fortes (Q18) e fracos (Q19) do guia, bem como se há algo que desejasse alterar no guia (Q20). Essa última tem o intuito de aprimorar o guia para uma segunda versão, ao passo que busca informações acerca do conteúdo, da estética, da compatibilidade e da escalabilidade.

Tabela 6.2: Perguntas relativas ao processo de validação.

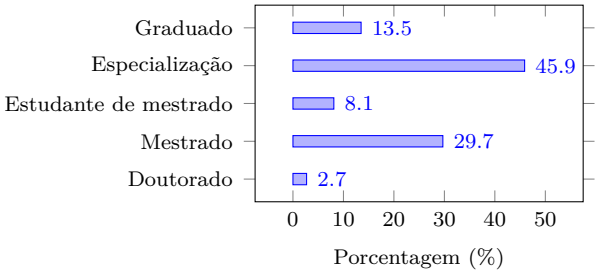
ID	Pergunta	Escala de resposta
Q09	Usar o guia de conformidade com a privacidade me ajudaria a cumprir as leis de proteção de dados mais rapidamente.	Escala Likert (Concordo fortemente; concordo; não discordo nem concordo; discordo; discordo fortemente).
Q10	Usar o guia de conformidade com a privacidade tornaria mais fácil navegar pelas regulamentações de privacidade.	Escala Likert (Concordo fortemente; concordo; não discordo nem concordo; discordo; discordo fortemente).
Q11	Usar o guia de conformidade com a privacidade me ajudaria a garantir uma melhor proteção da privacidade dos usuários.	Escala Likert (Concordo fortemente; concordo; não discordo nem concordo; discordo; discordo fortemente).
Q12	Usar o guia de conformidade com a privacidade ajudaria a melhorar a eficiência geral da conformidade com a privacidade em minha organização.	Escala Likert (Concordo fortemente; concordo; não discordo nem concordo; discordo; discordo fortemente).
Q13	Eu usaria o guia de conformidade com a privacidade para aprimorar as práticas de privacidade em meu trabalho.	Escala Likert (Concordo fortemente; concordo; não discordo nem concordo; discordo; discordo fortemente).
Q14	Eu acho o guia de conformidade com a privacidade fácil de usar.	Escala Likert (Concordo fortemente; concordo; não discordo nem concordo; discordo; discordo fortemente).
Q15	Eu acho o guia de conformidade com a privacidade claro e compreensível.	Escala Likert (Concordo fortemente; concordo; não discordo nem concordo; discordo; discordo fortemente).
Q16	Eu acho o guia de conformidade com a privacidade adaptável a diferentes estruturas e leis de privacidade (por exemplo, LGPD, GDPR).	Escala Likert (Concordo fortemente; concordo; não discordo nem concordo; discordo; discordo fortemente).
Q17	Eu acredito que o guia de conformidade com a privacidade exige muito conhecimento prévio sobre leis de privacidade para ser completamente compreendido.	Escala Likert (Concordo fortemente; concordo; não discordo nem concordo; discordo; discordo fortemente).
Q18	Em sua opinião, quais são os pontos fortes do guia de conformidade com a privacidade?	Em aberto.
Q19	Em sua opinião, quais são os pontos fracos do guia de conformidade com a privacidade?	Em aberto.
Q20	Existe algo que você mudaria no guia de conformidade com a privacidade? Se sim, por favor, explique o que mudaria.	Em aberto.

6.3 Resultados do Survey

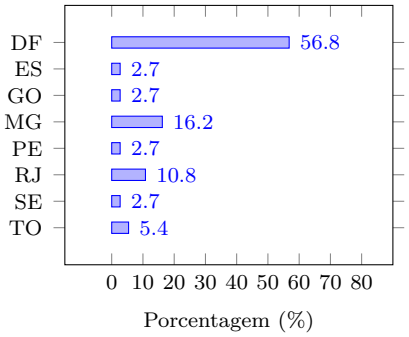
O questionário aplicado em duas turmas focalizadas em segurança e privacidade de dados obteve 37 respostas e foi utilizada análise de frequência para as perguntas estabelecidas na Tabela 6.1, com resultados elucidados na Figura 6.1. Dessa forma, os participantes variam em oito Estados, sete categorias de organização e dez áreas de trabalho, conforme Figuras 6.1b, 6.1c e 6.1e.

Com relação ao nível de escolaridade, uma vez que se tratavam de turmas de pós-graduação, a categoria de graduando não foi contemplada. Dessa forma, a maioria dos respondentes possuíam uma especialização (45,9%) ou mestrado (29,7%) — Figura 6.1a — e, em um maior escopo, 86,5% dos participantes possuíam uma pós-graduação.

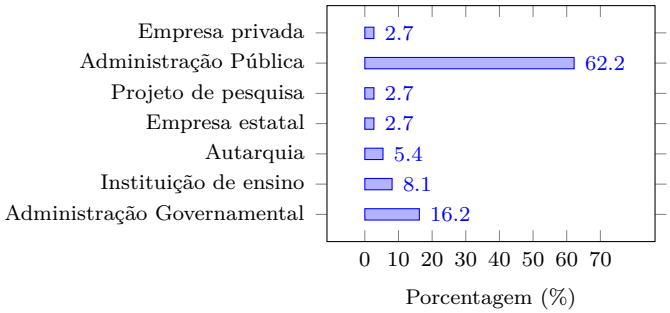
Já com relação à área de trabalho, foram estipuladas inicialmente dez categorias, conforme consta no Zenodo [66]. As categorias buscavam abranger o máximo possível de cargos relacionados à segurança, proteção e privacidade de dados pessoais. Todavia, os participantes apresentaram uma maior variabilidade, em que se fez necessário a criação de seis novas categorias: Gestão e Governança de TI (gerente de governança, diretor de TI, gestor de infraestrutura de TI e chefe de divisão); Compliance (coordenador de compliance e equipe do encarregado); Operações de TI (técnico e analista de TI, além de infraestrutura e segurança); Coordenador de auditoria interna; Analista de informações;



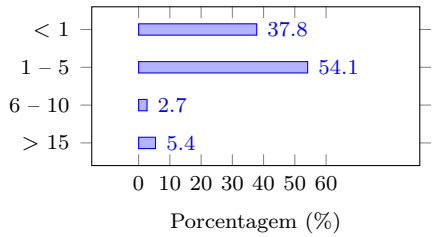
(a) Nível de escolaridade.



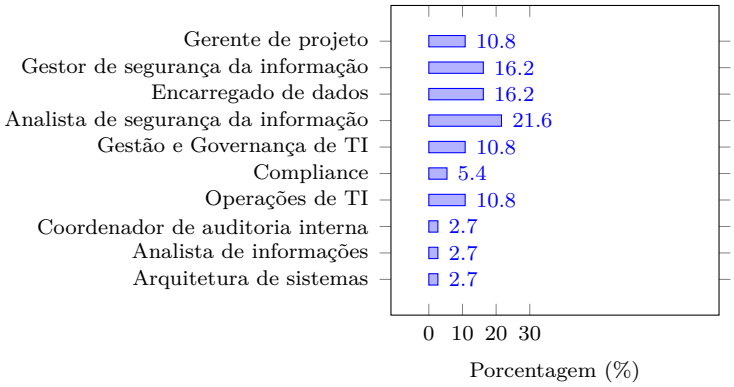
(b) Estado.



(c) Natureza da organização.



(d) Experiência.



(e) Área de trabalho.

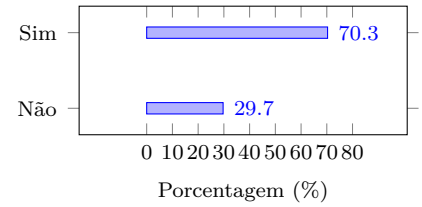
Figura 6.1: Perfil do participante: dados demográficos.

e Arquitetura de sistemas. A área de atuação dos participantes mostrou-se variada e balanceada (vide Figura 6.1e), de modo que a maior parte é referente à Analista de segurança da informação (21,6%).

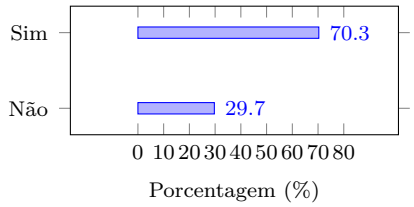
Acerca da localidade e origem da organização, pouco mais da metade (56,8%) dos respondentes residem no Distrito Federal (DF), como consta na Figura 6.1b e a grande maioria (62,2%) é empregado da Administração Pública (vide Figura 6.1c).

No que se refere à experiência na área de privacidade de dados, a maior parcela dos

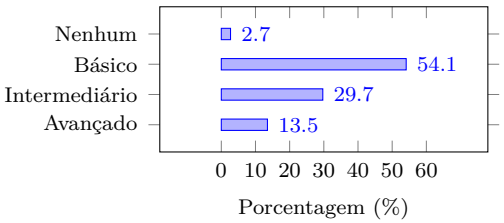
respondentes (54,1%) apresenta de 1 a 5 anos, enquanto que quase 92% situa-se na categoria abaixo de 6 anos de experiência nessa área, como consta na Figura 6.1d. Já com relação à experiência com leis de privacidade de dados, a Figura 6.2 explicita os resultados das questões Q06, Q07 e Q08.



(a) Pesquisou ou trabalhou previamente com leis.



(b) Pesquisa ou trabalha atualmente com leis.



(c) Nível de experiência com leis.

Figura 6.2: Perfil do participante: experiência em leis de proteção de dados.

É possível observar que, tanto para experiência prévia (Figura 6.2a), quanto para atual (Figura 6.2b), a maioria dos participantes (70,9%) apresenta certo conhecimento a respeito das diretrizes. Já com relação ao nível de experiência com leis, os participantes apresentam — em sua maioria — um nível básico (54,1%) ou avançado (29,7%), vide Figura 6.2c.

Acerca da validação do guia quando se trata de usabilidade, a Figura 6.3 aponta que cerca de 78,4% dos respondentes concordam — em algum nível — que o guia contribuiria para garantir a conformidade com as leis de proteção de dados pessoais mais rapidamente (Q09), e uma maioria expressiva de 91,9% concordam que o guia facilita a navegação em leis de privacidade (Q10). A navegação do guia foi um ponto forte detalhado pelos participantes, em conjunto da disposição facilidade dos dados (principalmente nas seções de Princípios e Direitos).

Para uma implementação prática, 78,4% apontaram que o guia seria de bom auxílio para melhorar a proteção da privacidade dos usuários (Q11) e a mesma parcela com relação à contribuição do guia para a melhora da conformidade com a privacidade na organização em que trabalham (Q12). Alguns participantes informaram que, pelo nível

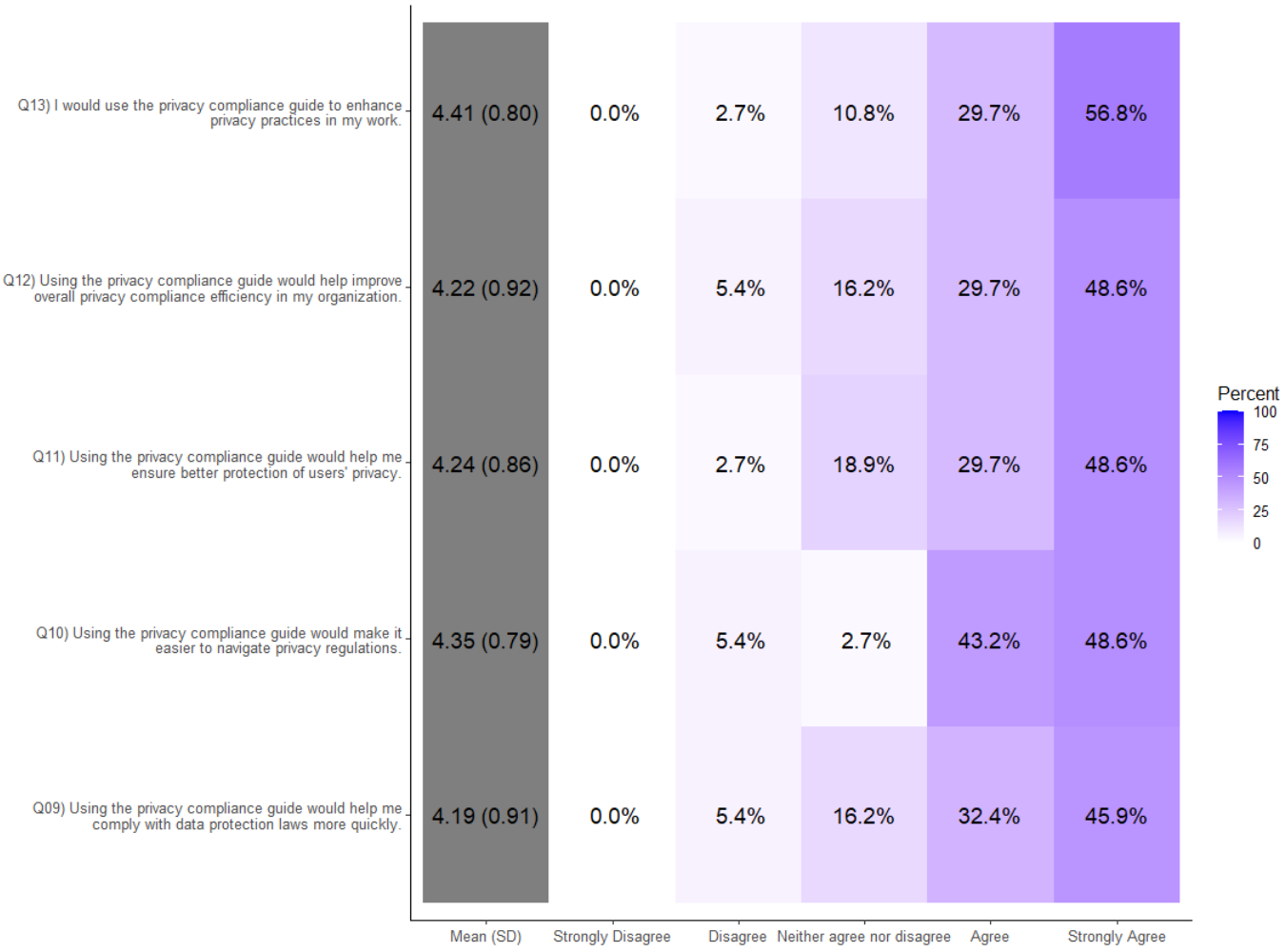


Figura 6.3: Avaliação de usabilidade de acordo com os participantes.

de generalização do guia — ao buscar atender o máximo de organizações possível —, poderia ser complicado a sua adaptação para empresas específicas, como as que dispõem de menor recurso financeiro.

Com base nisso, aproximadamente 86,5% dos respondentes afirmaram que usariam o guia para aprimorar as práticas de privacidade em seus respectivos trabalhos (Q13). Exemplificações no texto do guia com situações cotidianas poderiam contribuir para o aumento dessa taxa.

Já com relação à facilidade de uso, a Figura 6.4 explicita que 71,8% dos participantes consideram o guia de conformidade com a privacidade fácil de utilizar (Q14), além de que uma maior parte ainda — 78,4% — declara que o guia é claro e compreensível (Q15). Isso reflete o intuito principal em se elaborar esse mapeamento, uma vez que é a motivação do trabalho simplificar o campo das legislações e propor uma implementação facilitada.

Além disso, 71,8% dos respondentes concordam que o guia é escalável para diferentes

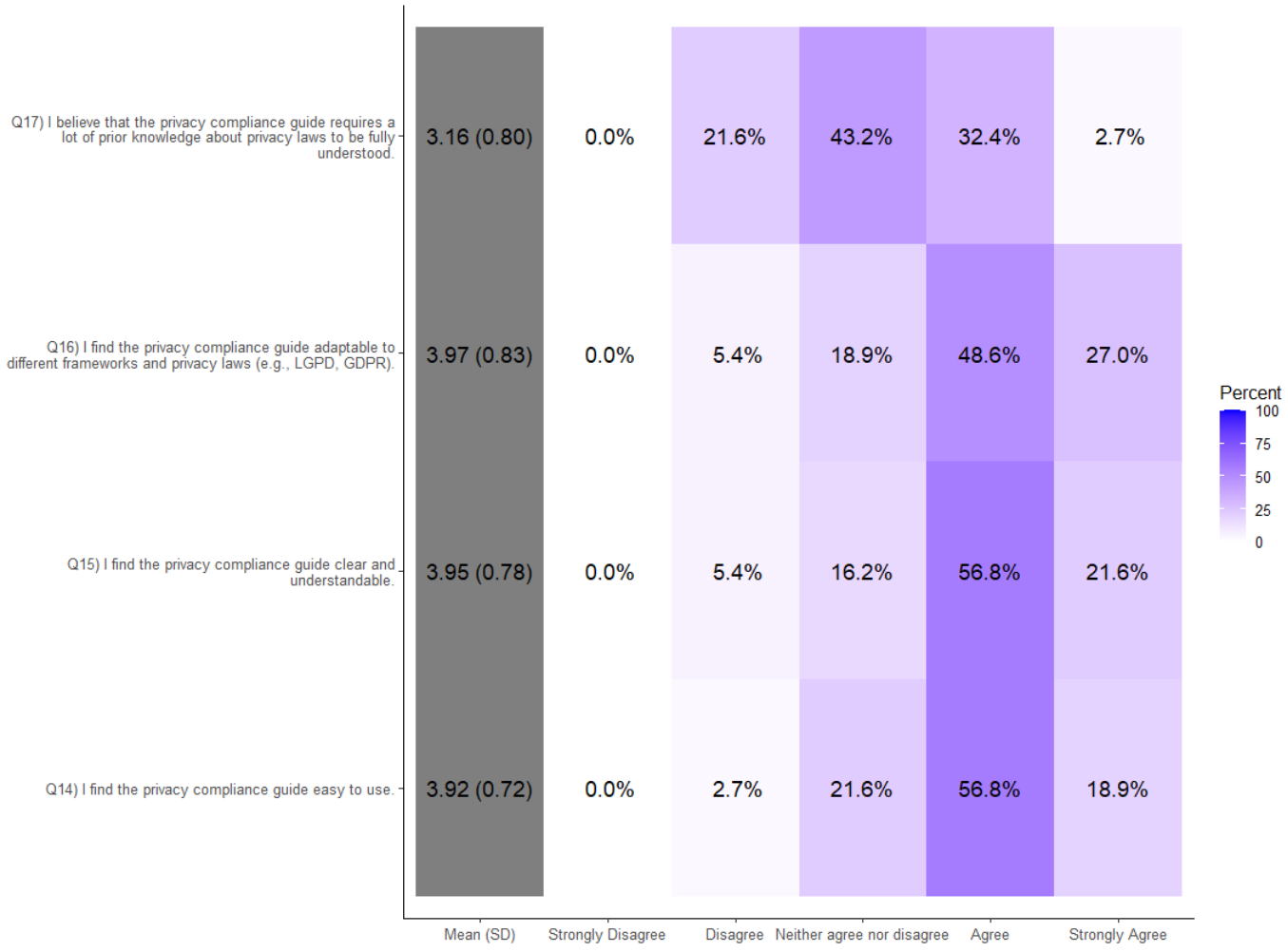


Figura 6.4: Avaliação de facilidade de uso de acordo com os participantes.

frameworks e legislações (Q16), de modo que favorece a proposta de incluir cada vez mais diretrizes. Todavia, o maior ponto fraco do guia apontado pelos respondentes foi a utilização de termos muito específicos — tratados pelas legislações —, de modo que requer conhecimento prévio acerca das legislações para ser completamente entendido (Q17).

Com relação aos pontos fortes do guia (Q18), o tópico mais citado pelos respondentes foi o de facilidade de compreensão e clareza, dado que é proposto um instrumento que busca comparar legislações complexas ao passo que mantêm a clareza da metodologia e dispõem as referências. Além disso, outros aspectos como aplicabilidade em organizações, interatividade por meio da gamificação (seções de princípios e direitos) e conscientização acerca dos temas tratados em privacidade de dados foram citados pelos participantes. A Tabela 6.3 apresenta os principais pontos fortes informados pelos respondentes, em que pelo menos três participantes elucidaram esses tópicos, além de exemplificações das transcrições.

Tabela 6.3: Transcrições dos participantes acerca dos pontos fortes do guia.

Pontos fortes	**Transcrições**
Facilidade de compreensão e Clareza	"Essa abordagem inovadora facilita a assimilação do conteúdo, tornando o aprendizado mais dinâmico e eficaz." "Facilidade de visualização das informações, acesso as informações e abrangência de fontes de consulta." "Acesso, linguagem fácil e sem uso de termos técnicos que dificultam a compreensão."
Aplicabilidade	"Essas estratégias ajudam as organizações a garantir a conformidade legal e a promover uma cultura de proteção de dados." "Ao abordar diretamente as dificuldades que as organizações encontram, como restrições orçamentárias e ambiguidades legais, o guia se torna uma ferramenta relevante e aplicável no cotidiano das equipes de trabalho." "Os pontos fortes de um guia de conformidade com a privacidade são: [...] flexibilidade para adaptação, capacitação contínua dos funcionários."
Interatividade	"A inclusão de um jogo interativo, que permite aos usuários explorar diretrizes de privacidade de forma lúdica, não apenas engaja os participantes, mas também promove uma compreensão mais profunda de como diferentes frameworks podem atender aos requisitos legais." "Gostei do modo de apresentação das informações e da forma de interação que foi apresentado nas abas Principles e Rights." "A possibilidade de utilizar os cartões para selecionar os princípios de privacidade da ISO."
Conscientização	"O guia enfatiza a educação e a conscientização sobre a privacidade, promovendo uma cultura organizacional responsável em relação à proteção de dados." "Os pontos fortes de um guia de conformidade com a privacidade incluem: [...] Foco na educação e conscientização dos colaboradores." "Colabora para disseminar a importância da privacidade."
Acesso Simplificado	"Facilita a navegação pelas normas de privacidade." "Claro, direto, conciso e permite comparar rapidamente as legislações existentes em outros países." "A ideia do guia é excelente pois sintetiza em um único local as informações sobre as principais regulamentações sobre o assunto."

Já acerca dos pontos fracos do guia (Q19) e as melhorias recomendadas (Q20), o principal tópico abordado pelos respondentes foi a de possível complexidade para iniciantes. Isso se deve ao fato de que, por meio da utilização de termos presentes nas legislações — técnicos —, há requisição de um certo nível de conhecimento prévio. Esse problema poderia ser mitigado com a introdução de um dicionário de termos no guia, como um glossário, em que seria possível compreender o contexto do termo utilizado por meio de linguagem simples.

Outros pontos fracos são referentes à falta de uma versão em português do guia e acerca da generalização e falta de exemplo de casos de uso. Os pontos fracos e respectivas melhorias estão explicitados na Tabela 6.4.

Tabela 6.4: Transcrições dos participantes acerca dos pontos fortes do guia.

Pontos fracos e melhorias	**Transcrições**
Complexidade para iniciantes	"Necessidade do usuário em entender as diferenças entre as leis dos países." "Acredito que algumas informações poderiam estar estruturadas de tal forma que trouxesse enfase na LGPD como ponto de partida." "O guia também pressupõe uma compreensão básica de termos legais e técnicos, o que pode ser uma barreira para não especialistas."
Idioma em português	"Falta uma opção para o português, já que se trata do uso de regulamentação brasileira." "Poderia ter uma tradução para o português." "Como foi uma pesquisa aplicada no Brasil e também se baseia na LGPD, senti falta de estar disponível em português."
Generalização	"Abordagem genérica, falta personalização para os diferentes tipos de organizações." "Enfoque genérico, sem considerar necessidades específicas." "A dificuldade de atender a todos os órgãos."
Exemplificação	"Incluir exemplos práticos do mundo real e estudos de caso sobre como organizações superam os desafios." "[...] inclusão de exemplos práticos e estudos de caso." "Exemplificar/prática."

6.4 Melhorias no Guia

Com relação as respostas abertas dos participantes à pesquisa, foram realizadas pequenas alterações e três adições significativas ao guia. Acerca das alterações menores, houveram correções textuais e enfoque em termos importantes que não alteram o sentido do guia,

meramente para uma melhor clareza e fluidez da leitura. Adicionalmente, foi inserida a frase “Este guia visa apoiar organizações de vários tamanhos na navegação pelas regulamentações de privacidade de dados, fornecendo práticas essenciais sem se aprofundar em detalhes técnicos extensos ou nuances específicas do setor.” na introdução, com o intuito de informar a generalização do guia e suas intenções.

Em relação às adições significativas, a primeira busca solucionar o problema da elevada complexidade para iniciantes. Para isso, foi implementado um glossário interativo em que, ao passar o mouse sobre termos muito técnicos ou novidades para principiantes, é exibida uma caixa que explica brevemente o significado.

Em seguida, na seção “About”, foi adicionado um exemplo contínuo de utilização do guia, com o intuito de fornecer um contexto claro de como utilizar a gamificação do guia para situações cotidianas. Por fim, também foi elaborada uma versão em português brasileiro do guia, disponível em `https://xdalle.github.io/5L2FGuide-PT-BR-/index.html` e o código-fonte aberto disponível em `https://github.com/xDalle/5L2FGuide-PT-BR-`. Essas melhorias buscam tornar o guia uma ferramenta mais acessível e útil para todos os públicos.

6.5 Síntese deste Capítulo

Este capítulo detalhou a metodologia e os resultados da validação do guia de conformidade com a privacidade. Duas turmas focalizadas na áreas de segurança, privacidade e proteção de dados foram convidadas para responder a uma pesquisa com o intuito de avaliar se o guia é útil e fácil de usar, além de coletar sugestões para aprimorar esses aspectos, caso necessário. Os resultados da pesquisa revelaram pontuações satisfatórias em relação à usabilidade e compreensão do guia. Além disso, os participantes contribuíram com sugestões que foram posteriormente adicionadas ao guia, como a adição de exemplos contínuos, um glossário interativo para esclarecer termos técnicos e a inclusão de uma versão em português brasileiro do guia.

Capítulo 7

Discussão

Neste capítulo é discutido os resultados obtidos nesse trabalho, com examinações acerca de suas implicações, contribuições teóricas, ameaças a validade das técnicas utilizadas e preocupações futuras.

7.1 Contribuição Teórica

Assim como explanado na Subseção 2.3, há diferentes enfoques com relação aos trabalhos relacionados: meramente comparação entre legislações (em variados níveis); somente apresentação dos desafios organizacionais ao entrar em conformidade com as leis; e ambas. A Tabela 7.1 elucida as principais diferenças entre este trabalho e os trabalhos relacionados.

Legislações abordadas nos trabalhos correlatos	[25]	[4]	[43]	[23]	[45]	[13]	[24]	[18]	[14]	Neste estudo
LGPD					x		x	x	x	x
GDPR	x	x	x	x	x	x	x	x	x	x
ADPPA										x
Australian Privacy Act	x			x						x
Privacy by Design	x	x		x	x		x			x
ISO/IEC 29100				x	x	x		x	x	x
Comparações entre Leis	x			x	x	x		x	x	x
Desafios organizacionais	x	x	x		x	x	x	x		x

Tabela 7.1: Comparativo entre trabalhos relacionados e o trabalho proposto.

Por meio dos resultados foi possível elaborar um guia prático e acessível para profissionais da área e, consequentemente, complementando estudos anteriores que apresentam comparações entre as leis e desafios específicos. A título de exemplo, estudos como [45], [13] e [18] discutem tanto comparações entre leis quanto desafios enfrentados pelas organizações, todavia há um enfoque em apenas uma área das legislações (princípios ou direitos), sem que haja um aprofundamento nas técnicas de conformidade ou na integração de múltiplos frameworks.

Além disso, estudos como [25], [23] e [24] estão muito mais alinhados com a proposta do trabalho, no quesito comparativo, uma vez que utilizam técnicas de codificação para

mapear os requisitos. Porém, o atual trabalho se diferencia ao explorar as situações de escopo, definições e sanções abordadas pelas legislações, além de integrar práticas do Privacy by Design e framework ISO. Dessa forma, o guia busca atender às necessidades específicas dos desenvolvedores e suas respectivas organizações, através do fornecimento de orientações práticas e detalhadas para alcançar a conformidade de maneira eficaz e interativa.

7.2 Preocupações Futuras

É inevitável a constante evolução das tecnologias e práticas relacionadas à proteção de dados pessoais, que são motivadas por inovações tecnológicas. Em consequência disso, o guia desenvolvido para essa pesquisa pode necessitar de revisões futuras para que permaneça relevante e eficaz, como qualquer ferramenta volátil à questão temporal.

Inicialmente, como discutido no Capítulo 4, um ponto de preocupação é um desafio exaltado pelos respondentes do survey, que são as constantes mudanças na lei (QD3). À medida que essas leis se adaptam para responder a problemas emergentes, as diretrizes e frameworks de conformidade podem se tornar insuficientes. Dessa forma, seria necessária a inclusão, no guia, de novas práticas recomendadas, que condizem com as novas realidades regulatórias.

Além disso, não só as legislações são passíveis de alterações, mas também as organizações. Isso quer dizer que, conforme há adoção de novas tecnologias, novos desafios poderão surgir quanto ao tratamento de dados pessoais. Por outro lado, obstáculos que antes existiam podem ser automaticamente solucionados pela inclusão de novas tecnologias. Em ambas situações, é necessário adaptar o guia para refletir práticas organizacionais atualizadas.

Por fim, os frameworks de privacidade também são passíveis de revisões significativas para alinhar às necessidades tecnológicas. Logo, isso poderia impactar a validade do guia, que trabalha com o Privacy by Design e ISO/IEC 29100. É possível que seja necessário a revisão dos mesmos quanto ao suporte oferecido e, caso necessário, a inclusão de novos frameworks que melhor atendam ao contexto. Além disso, a aplicação do guia em cenários práticos, especialmente em processos de desenvolvimento de software, constitui um caminho promissor para trabalhos futuros.

7.3 Ameaças a Validade

Para relatar as potenciais ameaças a validade do estudo e, consequentemente, as estratégias de mitigação, foi utilizada a metodologia proposta por Wholin et al. [101] em todas

as técnicas utilizadas. As classes de ameaça são explicitadas conforme a seguinte categorização: Validade Interna (ameaças que comprometem a conclusão sobre uma possível relação causal entre o tratamento e o resultado); Validade Externa (ameaças que limitam a capacidade de generalizar os resultados do experimento para o contexto industrial); Validade de Construção (ameaças que afetam a generalização do resultado do experimento para os conceitos ou teorias que há pretensão de medir); e Validade de Conclusão (ameaças que comprometem a capacidade de tirar conclusões corretas acerca das relações entre o tratamento e o resultado do experimento).

7.3.1 Revisão Sistemática de Literatura (RSL)

- Validade Interna: O estudo pode apresentar viés de seleção, uma vez que nem todos os artigos que tratam de comparações entre leis e desafios de conformidade das organizações podem ser incluídos e, dessa forma, pode ter um impacto direto no resultado da RSL. Para mitigar a ameaça, o processo de seleção dos estudos foi realizado por duas pessoas para múltiplas bases digitais, com critérios de inclusão e exclusão bem definidos — inclusive no snowball —, a fim de que houvesse uma vasta escolha de artigos relacionados. Ademais, o viés histórico é um fator relevante ao lidar com legislações, visto que é um meio de constante mudança. Dessa forma, foram incluídos apenas estudos publicados a partir de 2018 — ano em que a GDPR entrou em vigor e houve a aprovação da LGPD —, com enfoque nas mudanças legislativas ao longo do período.

- Validade Externa: Uma grande ameaça, quando se trata de RSL, é a interação entre história e tratamento, isto é, a depender da data de publicação de um estudo e do contexto temporal, normas de privacidade e de proteção de dados poderiam ser mais flexíveis ou mais rígidas. Para mitigar tal ameaça, foi evidenciado os limites de cada uma das legislações, bem como motivações culturais e históricas.

- Validade de Construção: A explicação inadequada pré-operacional dos construtos é uma ameaça da RSL, uma vez que os estudos podem possuir apresentação de termos semelhantes, mas com definições diferentes ou equivocadas. Para mitigar essa ameaça, foi realizada uma revisão em pares e subsequente codificação das informações, especialmente na etapa de comparação das legislações. Em relação às perguntas de pesquisa, é evidente um viés de método único, uma vez que se pode estabelecer uma conclusão prévia baseada apenas na RSL. Para mitigar a ameaça, em relação à RQ.1, o método de framework analysis funcionará como um complemento e validação dos resultados da RSL e, para RQ.2, o survey é realizado como validação dos desafios para o contexto brasileiro, semelhantemente. Ainda com relação às perguntas de

pesquisa e o protocolo da RSL, não há como garantir que a seleção de sinônimos para termos como “desafios” e “oportunidades” foi realizada de forma exaustiva. A técnica de snowball corroborou para redução dessa ameaça, uma vez que ampliou a busca para incluir estudos que possam ter utilizado terminologias diferentes.

- Validade de Conclusão: Para a maioria das RSL, o baixo poder estatístico é uma relevante ameaça, dado que a escolha de uma pequena quantidade de artigos pode acarretar em conclusões errôneas. Para mitigar no estudo, além da seleção de estudos base, o snowball apresentou uma boa alternativa para expandir a quantidade de estudos relacionados. Ademais, a confiabilidade das medidas e da implementação do tratamento são ameaças, principalmente quando o estudo é realizado por mais de uma pessoa. Para mitigá-las, todo o processo — desde a coleta até a codificação dos dados — foi padronizado e os resultados da extração apresentados em tabela.

7.3.2 Questionários

- Validade Interna: Uma ameaça de viés de seleção é evidente ao aplicar um survey, isto é, não é possível garantir que a escolha dos participantes é completamente aleatória, dado que a divulgação foi realizada por meio de redes sociais, para respondentes com escolaridade e localidade possivelmente semelhantes. Para mitigar essa ameaça, múltiplas plataformas foram utilizadas para a divulgação, no intuito de diversificar os participantes. Além disso, na elaboração de um survey, a ameaça de maturação é relevante quando a pesquisa é de longa duração, de modo que os participantes não possuam o mesmo interesse em responder as perguntas no decorrer do experimento. Para mitigar essa ameaça, optou-se para que a maior parte das questões do survey fosse de resposta rápida, isto é, múltipla escolha ou em escala Likert, em detrimento de resposta em aberto.

- Validade Externa: A interação entre seleção e tratamento é um fator relevante a ser considerado no survey, uma vez que as respostas dos participantes não necessariamente servirão para generalizar os desafios de todos os desenvolvedores e das organizações, ou os pontos fortes e fracos do guia. Para mitigar essa ameaça, foi realizado um agrupamento por meio dos perfis dos participantes — escolaridade, área de atuação, etc. — a fim de correlacionar o resultado com a experiência dos respondentes.

- Validade de Construção: Semelhantemente à questão da Validade Externa, as respostas dependerão de diversos aspectos do participante (construtos e níveis de construtos conflitantes) e, para resolver essa ameaça, múltiplas perguntas foram

esquematizadas para traçar o perfil do participante. Além disso, um viés de mono-operação é identificado quando há apenas um conjunto limitado de alternativas e o participante pode não se identificar com elas. Assim, em questões que tratavam de desafios e do perfil do participante, foi adicionada uma alternativa "outro", para que o respondente pudesse incluir o que fosse necessário, e para a validação do guia foram adicionadas perguntas de resposta livre para discussão dos pontos fortes e fracos o guia. Além disso, a confiabilidade das medidas é uma ameaça na estruturação de um survey, de modo que existe um viés de resposta extremada, isto é, os participantes tendem a optar por respostas que estão na extremidade da escala Likert. Para mitigar essa ameaça, a maior parte das perguntas era respondida em múltipla escolha ou em espaço aberto, além de uma complementação em perguntas de resposta livre para esse caso. Por fim, por se tratar de um questionário online, as perguntas não apresentavam intervenção do avaliador, ou seja, os participantes poderiam não incluir as respostas desejadas (ameaça de apreensão de avaliação). Para mitigar essa ameaça, no começo do survey foi elucidado que a participação não era obrigatória e, em qualquer situação, não era exigido que os respondentes completassem o questionário, a menos que fosse de espontânea vontade.

- Validade de Conclusão: Igualmente ao estabelecido na RSL, é necessário que o survey possua uma alta quantidade de respondentes, a fim de evitar a ameaça de baixo poder estatístico. Dessa forma, para reduzir esse problema no survey dos desafios de conformidade, buscou-se coletar pelo menos 100 respostas, a fim de que o tamanho da amostra pudesse ser expressivo. Já para o survey de validação do guia, a estratégia utilizada foi garantir uma amostragem mais eficiente, por meio da seleção de grupos que são mais relevantes para o estudo (alunos de segurança, proteção e privacidade de dados). Além disso, uma ameaça à validade de conclusão pode surgir da interpretação subjetiva dos resultados pelos pesquisadores. Para mitigar essa ameaça, o processo de análise dos dados foi estruturado com diretrizes claras e reprodutíveis, disponibilizadas por meio do Zenodo [66]. Assim, sempre que possível, as análises foram realizadas com base em critérios objetivos, seguindo a técnica de teoria fundamentada.

7.3.3 Elaboração do Guia

- Validade Interna: Para a aplicação do guia em um contexto prático, duas ameaças surgem como adversas: seleção e difusão ou imitação de tratamentos. Isso quer dizer que, no caso de uma maior especificação do guia para determinados setores, é possível que o mesmo não seja representativo e, em contrapartida — caso em que o

guia propõe abordagens gerais para todos os setores —, as organizações podem ter problemas em tentar imitar os métodos de setores que não são adequados para o seu contexto. Para mitigar isso, há uma busca por diversificar as fontes de dados, de modo que a amostra seja a mais ampla possível e, ao mesmo tempo, o guia informa essas generalizações e há recomendações para diversos cenários acerca dos desafios de conformidade. Acerca da história e maturação, como informado na subseção 7.2, o guia é sensível ao tempo, de modo que tanto os estudos anteriores quanto as leis poderão afetar a aplicabilidade de suas diretrizes, ao longo do tempo. Isso pode ser mitigado por meio da constante atualização do guia, a fim de garantir que ele esteja a par de mudanças legislativas significativas.

- Validade Externa: Assim como no contexto de Validade Interna, há uma ameaça quando se trata da interação da história e tratamento, dado que as condições temporais afetam a aplicabilidade dos resultados do guia. A técnica mais viável de mitigação é a mesma, isto é, constantes atualizações e revisões, para refletir o contexto mais atual. Há também uma ameaça acerca da interação da seleção e tratamento, dado que o guia deve ser inclusivo para quaisquer organizações. Assim, a RSL buscou identificar estudos que trabalhassem com diversas empresas — pequenas, médias e grandes —, a fim de que as técnicas do guia sejam aplicáveis para variados cenários.

- Validade de Construção: Na parte teórica, existe uma ameaça que se trata da explicação inadequada dos construtos, ou seja, deve-se garantir que as definições apresentadas no guia são entendidas pelo leitor. Para mitigar, como proposto pela validação, foi incluído o glossário interativo em conceitos específicos do escopo de leis de privacidade. Com relação ao viés de método único, a validação do guia é realizada por survey, a fim de adequar e aperfeiçoar o guia para os usuários. Além disso, a construção do guia proporciona a ameaça de expectativas do experimentador, que pode ser mitigada pela fiscalização de múltiplos participantes (três, no caso). Por fim, para evitar a ameaça de adivinhação de hipótese, o guia proporciona técnicas claras e objetivas, bem como o contexto em que foram utilizadas (e motiva o leitor a adicionar novas, caso seja necessário).

- Validade de Conclusão: Assim como o discutido na RSL, a elaboração do guia leva em conta a ameaça de baixo poder estatístico, uma vez que uma amostragem pequena de estudos poderiam levar a conclusões equivocadas. Logo, a técnica de snowball contribui também para a mitigação dessa ameaça. Além disso, a confiabilidade das medidas é uma ameaça a ser considerada, dado que a categorização dos temas das tabelas dependem de interpretações consistentes. Para mitigar essa ameaça, o

processo framework analysis e suas etapas foram seguidos precisamente, inclusive com a contribuição de três pesquisadores da Universidade Federal de Pernambuco (UFPE), sendo um graduando em Ciência da Computação, um doutorando em Ciência da Computação com foco em LGPD e profissionais de Internet das Coisas, e uma pós-doutora em Ciência da Computação, especializada em Direito Digital e Proteção de Dados, além de atuar como advogada na área de Segurança da Informação e LGPD. A colaboração desses pesquisadores, com diferentes perfis e especializações, foi fundamental para garantir maior confiabilidade nas análises. Vale lembrar que as ameaças relativas à RSL e ao survey também se aplicam nessa etapa, dado que o guia foi elaborado a partir dos mesmos.

7.4 Síntese deste Capítulo

Este capítulo sintetizou as contribuições teóricas da pesquisa, isto é, o mapeamento comparativo das legislações e o guia desenvolvido para apoiar a conformidade com leis e frameworks de proteção de dados. O guia também fornece orientações práticas quanto aos desafios enfrentados pelos desenvolvedores no processo de conformidade legal. As preocupações futuras foram expostas com relação ao guia, como possíveis mudanças regulatórias, novos desafios organizacionais e evolução dos frameworks, que requerem atualizações periódicas do material proposto para manter a relevância e eficácia no contexto de proteção de dados. Por fim, as ameaças a validade das técnicas aplicadas pelo estudo foram expostas.

Capítulo 8

Conclusão

Neste trabalho foram apresentadas diversas legislações de privacidade de dados que são utilizadas mundialmente — brasileira, europeia, estadunidense e australiana — e relevantes frameworks de privacidade — Privacy by Design e ISO/IEC 29100 — com o intuito de contextualizar conceitos e particularidades de cada uma das diretrizes.

A partir disso, foi realizada uma Revisão Sistemática de Literatura (RSL) focalizada na identificação de semelhanças e diferenças entre as legislações, além dos desafios e técnicas utilizadas por organizações para garantir a conformidade com as respectivas leis. Posteriormente, foi aplicada a metodologia de snowball, que possibilitou a detecção de estudos relacionados, a fim de agregar os resultados da RSL.

Como resultado da RSL, a GDPR é a legislação que apresenta maior maturidade e abrangência quando se trata de proteção de dados pessoais, seguida pela LGPD. Além disso, embora a ADPPA seja a mais recente, sua inspiração local na lei da Califórnia frequentemente coloca em prioridade aspectos econômicos, em detrimento do direito à privacidade. Por fim, a lei australiana — que é precursora das demais — apresenta o escopo menos abrangente dentre as discutidas. Quanto aos desafios de conformidade, a maior parte é relativa ao processo de compreensão e aplicação da lei, ou seja, conhecimento teórico (da legislação) e prático (de técnicas), com diversos desenvolvedores e organizações apresentando dificuldades nessas áreas. Em seguida, restrições orçamentárias e falta de materiais, de ferramentas e até mesmo padronização dos mesmos também foram identificados como grandes desafios.

Para validar os resultados obtidos pela RSL quando se trata das dificuldades das organizações, foi elaborado um survey que questiona desenvolvedores brasileiros quanto à essa problemática, ou seja, direcionado para a Lei Geral de Proteção de Dados Pessoais (LGPD) e seus desafios de conformidade. Por meio da prática de teoria fundamentada foi possível correlacionar os resultados obtidos no survey com os identificados na RSL, além de constatar outros novos desafios no contexto brasileiro e possíveis técnicas para solução.

Assim, foi elaborado um guia unificado com as legislações e frameworks desse estudo, por meio da técnica de framework analysis. As leis foram comparadas através da divisão em temas e os desafios identificados também foram incluídos no guia. O guia também apresenta a cobertura dos frameworks Privacy by Design e ISO/IEC 29100 com as legislações, com relação aos princípios e direitos. Para o processo de validação, o survey aplicado em turmas de segurança, privacidade e proteção de dados introduziu novas ideias de melhorias no guia, que foram registradas e implementadas.

Como trabalhos futuros, é interessante realizar entrevistas com os desenvolvedores de software, e realizar uma análise qualitativa, de modo que haja uma maior especialização sobre a implementação das técnicas abordadas no guia pela indústria. Além disso, é motivada a extensão do estudo para outras legislações de privacidade e frameworks de privacidade, uma vez que o objetivo principal é unificar e simplificar as soluções para os desafios de conformidade. Quanto ao guia, uma possibilidade é a especificação para setores específicos da indústria, que podem apresentar níveis de desafios distintos quando se trata da generalização do guia.

Referências

[1] Selim, Aybeyan: *Systematic review of big data, digital transformation areas and industry 4.0 trends in 2021.* International Scientific Journal Vision, 6(2):27–41, 2021. 1

[2] Lee, Sabinne e Kwangho Jung: *The impact of changing public service delivery on inappropriate payment error: From analogue paper coupon to digitalized electronic benefit transfer system.* Em Eom, Seok-Jin e Jooho Lee (editores): *dg.o '20: The 21st Annual International Conference on Digital Government Research, Seoul, Republic of Korea, June 15-19, 2020*, páginas 68–81. ACM, 2020. https://doi.org/10.1145/3396956.3398255. 1

[3] Tregua, Marco, Cristina Mele, Tiziana Russo Spena, Maria Luisa Marzullo e Adriana Carotenuto: *Digital transformation in the era of covid-19.* Em Leitner, Christine, Walter Ganz, Debra Satterfield e Clara Bassano (editores): *Advances in the Human Side of Service Engineering - Proceedings of the AHFE 2021 Virtual Conference on The Human Side of Service Engineering, July 25-29, 2021, USA*, volume 266 de *Lecture Notes in Networks and Systems*, páginas 97–105. Springer, 2021. https://doi.org/10.1007/978-3-030-80840-2_10. 1

[4] Machado, Pedro, Jéssyka Vilela, Mariana Maia Peixoto e Carla T. L. L. Silva: *A systematic study on the impact of GDPR compliance on organizations.* Em Cunha, Mônica Ximenes Carneiro da, Marcílio F. de Souza Júnior, Johnny Cardoso Marques, Tadeu Moreira de Classe e Rafael D. Araújo (editores): *Proceedings of the XIX Brazilian Symposium on Information Systems, SBSI 2023, Maceió, Brazil, 29 May 2023- 1 June 2023*, páginas 435–442. ACM, 2023. https://doi.org/10.1145/3592813.3592935. 1, 2, 3, 4, 29, 31, 42, 47, 48, 51, 52, 64, 69, 121

[5] Feng, Yun, Baoxu Liu, Xiang Cui, Chaoge Liu, Xuebin Kang e Junwei Su: *A systematic method on PDF privacy leakage issues.* Em *17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications / 12th IEEE International Conference On Big Data Science And Engineering, TrustCom/BigDataSE 2018, New York, NY, USA, August 1-3, 2018*, páginas 1020–1029. IEEE, 2018. https://doi.org/10.1109/TrustCom/BigDataSE.2018.00144. 1

[6] Carvalho, Artur Potiguara, Fernanda Potiguara Carvalho, Edna Dias Canedo e Pedro Henrique Potiguara Carvalho: *Big data, anonymisation and governance to personal data protection.* Em Eom, Seok-Jin e Jooho Lee (editores): *dg.o '20: The 21st Annual International Conference on Digital Government Research, Seoul,*

Republic of Korea, June 15-19, 2020, páginas 185–195. ACM, 2020. https://doi.org/10.1145/3396956.3398253. 1, 2

[7] Rocha, Lucas Dalle, Geovana Ramos Sousa Silva e Edna Dias Canedo: *Privacy compliance in software development: A guide to implementing the LGPD principles.* Em Hong, Jiman, Maart Lanperne, Juw Won Park, Tomás Cerný e Hossain Shahriar (editores): *Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing, SAC 2023, Tallinn, Estonia, March 27-31, 2023*, páginas 1352–1361. ACM, 2023. https://doi.org/10.1145/3555776.3577615. 1, 16, 43, 44, 48, 49, 50, 51, 52, 53, 67, 70, 72, 80

[8] Cambraia, Duda: *Em 2021, Brasil ficou no topo de vazamento de informação no mundo, diz especialista.* CNN, 2021. https://www.cnnbrasil.com.br/tecnologia/em-2021-brasil-ficou-no-topo-de-vazamento-de-informacao-no-mundo-diz-especialista/, acesso em 15/07/2023. 1

[9] Adhatarao, Supriya e Cédric Lauradoux: *Exploitation and sanitization of hidden data in PDF files: Do security agencies sanitize their PDF files?* Em Borghys, Dirk, Patrick Bas, Luisa Verdoliva, Tomás Pevný, Bin Li e Jennifer Newman (editores): *IH&MMSec '21: ACM Workshop on Information Hiding and Multimedia Security, Virtual Event, Belgium, June, 22-25, 2021*, páginas 35–44. ACM, 2021. https://doi.org/10.1145/3437880.3460405. 1

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

[11] Majeed, Abdul e Sungchang Lee: *Anonymization techniques for privacy preserving data publishing: A comprehensive survey.* IEEE Access, 9:8512–8545, 2021. https://doi.org/10.1109/ACCESS.2020.3045700. 2

[12] Brasil: *Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD).* Diário Oficial da República Federativa do Brasil, 2018. http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. 2, 3, 8, 9, 10, 11, 12, 13, 14, 16, 22, 23, 24, 25, 64, 78, 79, 81

[13] Sangaroonsilp, Pattaraporn, Hoa Khanh Dam, Morakot Choetkiertikul, Chaiyong Ragkhitwetsagul e Aditya Ghose: *A taxonomy for mining and classifying privacy requirements in issue reports.* Inf. Softw. Technol., 157:107162, 2023. https://doi.org/10.1016/j.infsof.2023.107162. 2, 3, 23, 28, 30, 42, 44, 45, 48, 121

[14] Ferrão, Sâmmara Éllen Renner, Geovana Ramos Sousa Silva, Edna Dias Canedo e Fabiana Freitas Mendes: *Towards a taxonomy of privacy requirements based on*

the LGPD and ISO/IEC 29100. Inf. Softw. Technol., 168:107396, 2024. https://doi.org/10.1016/j.infsof.2024.107396. 2, 31, 96, 98, 121

[15] Sirur, Sean, Jason R. C. Nurse e Helena Webb: *Are we there yet?: Understanding the challenges faced in complying with the general data protection regulation (GDPR)*. Em Hallman, Roger A., Shujun Li e Victor Chang (editores): *Proceedings of the 2nd International Workshop on Multimedia Privacy and Security, MPS@CCS 2018, Toronto, ON, Canada, October 15, 2018*, páginas 88–95. ACM, 2018. https://doi.org/10.1145/3267357.3267368. 2, 15, 42, 47, 48, 52, 72

[16] Ekambaranathan, Anirudh, Jun Zhao e George Chalhoub: *Navigating the data avalanche: Towards supporting developers in developing privacy-friendly children's apps*. Proc. ACM Interact. Mob. Wearable Ubiquitous Technol., 7(2):53:1–53:24, 2023. https://doi.org/10.1145/3596267. 3, 16, 22, 43, 48, 51, 52

[17] Davier, Thomas Serban Von, Konrad Kollnig, Reuben Binns, Max Van Kleek e Nigel Shadbolt: *We are not there yet: The implications of insufficient knowledge management for organisational compliance*. CoRR, abs/2305.04061, 2023. https://doi.org/10.48550/arXiv.2305.04061. 3, 15, 43, 45, 48, 49, 50, 66

[18] 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. 3, 4, 8, 16, 20, 25, 31, 42, 44, 45, 46, 47, 48, 49, 50, 53, 121

[19] Carvalho, Artur Potiguara, Edna Dias Canedo, Fernanda Potiguara Carvalho e Pedro Henrique Potiguara Carvalho: *Anonymisation and compliance to protection data: Impacts and challenges into big data*. Em Filipe, Joaquim, Michal Smialek, Alexander Brodsky e Slimane Hammoudi (editores): *Proceedings of the 22nd International Conference on Enterprise Information Systems, ICEIS 2020, Prague, Czech Republic, May 5-7, 2020, Volume 1*, páginas 31–41. SCITEPRESS, 2020. https://doi.org/10.5220/0009411100310041. 3, 9

[20] Hornuf, Lars, Sonja Mangold e Yayun Yang: *Data protection law in germany, the united states, and china*. Em *Data Privacy and Crowdsourcing: A Comparison of Selected Problems in China, Germany and the United States*, páginas 19–79. Springer, 2023. 3, 19

[21] Kaufmann, Julia, Felix Hilgert e Runa Wohlthat: *The proposed american data privacy and protection act in comparison with gdpr*. Computer Law Review International, 23(5):146–152, 2022. https://doi.org/10.9785/cri-2022-230505. 4, 13, 16, 17, 42, 44, 45

[22] Castro, Evandro Thalles Vale de, Geovana R. S. Silva e Edna Dias Canedo: *Ensuring privacy in the application of the brazilian general data protection law (LGPD)*. Em Hong, Jiman, Miroslav Bures, Juw Won Park e Tomás Cerný (editores): *SAC '22: The 37th ACM/SIGAPP Symposium on Applied Computing, Virtual Event, April*

25 - 29, 2022, páginas 1228–1235. ACM, 2022. https://doi.org/10.1145/3477314.3507023. 4, 13, 43, 45, 48

[23] Barth, Susanne, Dan Ionita e Pieter H. Hartel: *Understanding online privacy - A systematic review of privacy visualizations and privacy by design guidelines*. ACM Comput. Surv., 55(3):63:1–63:37, 2023. https://doi.org/10.1145/3502288. 4, 14, 22, 23, 25, 26, 30, 96, 98, 121

[24] 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. 4, 23, 31, 85, 121

[25] Aljeraisy, Atheer, Masoud Barati, Omer F. Rana e Charith Perera: *Privacy laws and privacy by design schemes for the internet of things: A developer's perspective*. ACM Comput. Surv., 54(5):102:1–102:38, 2022. https://doi.org/10.1145/3450965. 4, 15, 16, 22, 23, 25, 28, 31, 43, 45, 46, 47, 48, 50, 62, 80, 82, 83, 96, 98, 121

[26] Prodanov, Cleber Cristiano e Ernani Cesar De Freitas: *Metodologia do trabalho científico: métodos e técnicas da pesquisa e do trabalho acadêmico-2ª Edição*. Editora Feevale, 2013. 5

[27] Goldsmith, Laurie J: *Using framework analysis in applied qualitative research.* Qualitative Report, 26(6), 2021. 5, 75, 76

[28] Felizardo, Kátia Romero, Emilia Mendes, Marcos Kalinowski, Érica Ferreira de Souza e Nandamudi L. Vijaykumar: *Using forward snowballing to update systematic reviews in software engineering*. Em *Proceedings of the 10th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement, ESEM 2016, Ciudad Real, Spain, September 8-9, 2016*, páginas 53:1–53:6. ACM, 2016. https://doi.org/10.1145/2961111.2962630. 5, 39

[29] Chun Tie, Ylona, Melanie Birks e Karen Francis: *Grounded theory research: A design framework for novice researchers*. SAGE open medicine, 7:2050312118822927, 2019. 5, 58, 61

[30] Erickson, Abigayle: *Comparative analysis of the eu's gdpr and brazil's lgpd: Enforcement challenges with the lgpd*. Brook. J. Int'l L., 44:859, 2018. 8

[31] Voss, W Gregory: *The ccpa and the gdpr are not the same: why you should understand both*. W. Gregory Voss,'The CCPA and the GDPR Are Not the Same: Why You Should Understand Both,'CPI Antitrust Chronicle, 1(1):7–12, 2021. 8, 42, 44

[32] Gaydutschenko, Iwan: *Vazamentos de dados: uma análise a partir da lgpd e das políticas de compliance*, 2022. 9

[33] Sarlet, Gabrielle Bezerra Sales e Regina Linden Ruaro: *A proteção de dados sensíveis no sistema normativo brasileiro sob o enfoque da lei geral de proteção de dados (lgpd)–l. 13.709/2018*. Revista Direitos Fundamentais & Democracia, 26(2):81–106, 2021. 9

[34] Doneda, Danilo: *Da privacidade à proteção de dados pessoais: elementos da formação da lei geral de proteção de dados*. Revista dos Tribunais. São Paulo: Thomas Reuters Brasil, 2nd edição, 2020. 10, 11, 23

[35] Boeckl, Kaitlin R e Naomi B Lefkovitz: *NIST privacy framework: A tool for improving privacy through enterprise risk management, version 1.0*, 2020. https://doi.org/10.6028/NIST.CSWP.01162020pt. 10

[36] Cybersecurity, European Union Agency for: *Deploying Pseudonymisation Techniques The case of the Health Sector*, 2022. https://www.enisa.europa.eu/publications/deploying-pseudonymisation-techniques, acesso em 14/10/2023. 10

[37] Zibuschka, Jan, Sebastian Kurowski, Heiko Roßnagel, Christian H. Schunck e Christian Zimmermann: *Anonymization is dead - long live privacy*. Em Roßnagel, Heiko, Sven Wagner e Detlef Hühnlein (editores): *Open Identity Summit 2019, OID 2019, Garmisch-Partenkirchen, Germany, March 28-29, 2019*, volume P-293 de *LNI*, páginas 71–82. GI, 2019. https://dl.gi.de/handle/20.500.12116/20995. 11

[38] Aguilar Pereira Neves, Rebeca de: *GDPR e LGPD: Estudo comparativo*, 2021. https://repositorio.uniceub.br/jspui/handle/prefix/15239, acesso em 15/01/2024. 11, 42, 46, 48, 53, 80, 83

[39] Alomar, Noura e Serge Egelman: *Developers say the darnedest things: Privacy compliance processes followed by developers of child-directed apps*. Proc. Priv. Enhancing Technol., 2022(4):250–273, 2022. https://doi.org/10.56553/popets-2022-0108. 12, 43, 45, 48, 50, 52

[40] Brasil: *Lei nº 8.069, de 13 de julho de 1990. Estatuto da Criança e do Adolescente (ECA)*. Diário Oficial da República Federativa do Brasil, 1990. https://www.planalto.gov.br/ccivil_03/leis/l8069.htm. 13

[41] Parliament, The European e The Council: *General Data Protection Regulation (GDPR): EU Data Protection Rules*, 2018. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679, acesso em 14/10/2023. 13, 14, 15, 16, 22, 24, 79, 81

[42] Lorenzon, Laila Neves: *AnÁlise comparada entre regulamentaÇÕes de dados pessoais no brasil e na uniÃo europeia (lgpd e gdpr) e seus respectivos instrumentos de enforcement*. CENTRO DE EXCELÊNCIA JEAN MONNET DA FGV DIREITO RIO, 2021. https://hml-bibliotecadigital.fgv.br/ojs/index.php/rpdue/issue/view/4599, acesso em 15/01/2024. 13, 42, 44, 46

[43] Li, Ze Shi, Colin M. Werner, Neil A. Ernst e Daniela E. Damian: *Towards privacy compliance: A design science study in a small organization*. Inf. Softw. Technol., 146:106868, 2022. https://doi.org/10.1016/j.infsof.2022.106868. 13, 30, 31, 43, 44, 46, 48, 51, 53, 69, 121

[44] Starchon, Peter e Tomás Pikulík: *GDPR principles in data protection encourage pseudonymization through most popular and full-personalized devices - mobile phones*. Em Shakshuki, Elhadi M. e Ansar-Ul-Haque Yasar (editores): *The*

10th International Conference on Ambient Systems, Networks and Technologies (ANT 2019) / The 2nd International Conference on Emerging Data and Industry 4.0 (EDI40 2019) / Affiliated Workshops, April 29 - May 2, 2019, Leuven, Belgium, volume 151 de *Procedia Computer Science*, páginas 303–312. Elsevier, 2019. https://doi.org/10.1016/j.procs.2019.04.043. 14

[45] Canedo, Edna Dias, Angélica 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. https://doi.org/10.3390/e22040429. 14, 15, 30, 43, 45, 46, 48, 79, 80, 83, 121

[46] Ardabili, Babak Rahimi, Armin Danesh Pazho, Ghazal Alinezhad Noghre, Christopher Neff, Arun Ravindran e Hamed Tabkhi: *Understanding ethics, privacy, and regulations in smart video surveillance for public safety*. CoRR, abs/2212.12936, 2022. https://doi.org/10.48550/arXiv.2212.12936. 16, 19, 42, 45, 83

[47] Naqvi, Syed Khurram Hussain e Komal Batool: *A comparative analysis between general data protection regulations and california consumer privacy act*. Journal of Computer Science, Information Technology and Telecommunication Engineering, 4(1):326–332, 2023. 16, 43, 44, 45, 46, 83

[48] Matulytė, Raminta: *Comparing data protection regulation models of the eu and the us: which one is more preferred by the society?* Tese de Doutoramento, Vilniaus universitetas, 2022. 16, 17, 42, 44

[49] Union, Committee of the Whole House on the State of the: *American Data Privacy and Protection Act (ADPPA)*, 2022. https://www.congress.gov/bill/117th-congress/house-bill/8152/text, acesso em 14/10/2023. 17, 18, 19, 79, 80, 81

[50] Anwar, Memoona J., Asif Gill e Ghassan Beydoun: *A review of australian information privacy laws and standards for secure digital ecosystems*. Em *Australasian Conference on Information Systems, ACIS 2018, Sydney, NSW, Australia, 3-5 December 2018*, página 36, 2018. https://aisel.aisnet.org/acis2018/36. 20, 22, 43, 44, 45, 80, 83

[51] OAIC, Australian Government: *The Privacy Act*, 1988. https://www.oaic.gov.au/privacy/privacy-legislation/the-privacy-act, acesso em 14/10/2023. 20, 22, 80, 82

[52] OAIC, Australian Government: *Family Law Act 1975*, 1975. https://www.legislation.gov.au/C2004A00275/2019-03-10/text, acesso em 14/10/2023. 22

[53] Aljeraisy, Atheer, Masoud Barati, Omer F. Rana e Charith Perera: *Exploring the relationships between privacy by design schemes and privacy laws: A comparative analysis*. CoRR, abs/2210.03520, 2022. https://doi.org/10.48550/arXiv.2210.03520. 23, 27

[54] Cavoukian, Ann: *Privacy by design*, 2009. 23

[55] Secretary, ISO Central: *ISO/IEC 29100 : Information technology — security techniques — privacy framework*. Standard, International Organization for Standardization, Geneva, CH, 2011. 25, 26, 29

[56] Hassan, Fadi, David Sánchez, Jordi Soria-Comas e Josep Domingo-Ferrer: *Automatic anonymization of textual documents: Detecting sensitive information via word embeddings*. Em *18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications / 13th IEEE International Conference On Big Data Science And Engineering, TrustCom/BigDataSE 2019, Rotorua, New Zealand, August 5-8, 2019*, páginas 358–365. IEEE, 2019. `https://doi.org/10.1109/TrustCom/BigDataSE.2019.00055`. 27, 28

[57] Wong, Kok Seng, Nguyen Anh Tu, Dinh Mao Bui, Shih Yin Ooi e Myung Ho Kim: *Privacy-preserving collaborative data anonymization with sensitive quasi-identifiers*. Em *2019 12th CMI Conference on Cybersecurity and Privacy (CMI)*, páginas 1–6. IEEE, 2019. 28, 29

[58] Júnior, José Luiz de Moura Faleiros e Guilherme Magalhães Martins: *Proteção de dados e anonimização: Perspectivas à luz da lei nº 13.709/2018*. REI-REVISTA ESTUDOS INSTITUCIONAIS, 7(1):376–397, 2021. 29

[59] Basdekis, Ioannis, Christos Kloukinas, Carlos Agostinho, Ioannis Vezakis, Andreia Pimenta, Luigi Gallo e George Spanoudakis: *Pseudonymisation in the context of gdpr-compliant medical research*. Em *19th International Conference on the Design of Reliable Communication Networks, DRCN 2023, Vilanova i la Geltru, Spain, April 17-20, 2023*, páginas 1–6. IEEE, 2023. `https://doi.org/10.1109/DRCN57075.2023.10108370`. 28

[60] Nurgalieva, Leysan, Alisa Frik e Gavin Doherty: *A narrative review of factors affecting the implementation of privacy and security practices in software development*. ACM Comput. Surv., 55(14s), jul 2023, ISSN 0360-0300. `https://doi.org/10.1145/3589951`. 28, 43, 48, 51

[61] Kitchenham, Barbara, Stuart Charters *et al.*: *Guidelines for performing systematic literature reviews in software engineering*, 2007. 33, 36, 37

[62] Brereton, Pearl, Barbara A Kitchenham, David Budgen, Mark Turner e Mohamed Khalil: *Lessons from applying the systematic literature review process within the software engineering domain*. Journal of systems and software, 80(4):571–583, 2007. 35

[63] Ley, Michael: *The dblp computer science bibliography: Evolution, research issues, perspectives*. Em *International symposium on string processing and information retrieval*, páginas 1–10. Springer, 2002. 35

[64] Voigt, Dominik, Oliver Kopp e Karoline Wild: *Systematic literature review tools: Are we there yet?* Em *Proceedings of the 13th Central European Workshop on Services and their Composition (ZEUS 2021)*, páginas 83–88, 2021. 38

[65] Wohlin, Claes, Marcos Kalinowski, Kátia Romero Felizardo e Emilia Mendes: *Successful combination of database search and snowballing for identification of primary studies in systematic literature studies*. CoRR, abs/2307.02612, 2023. https://doi.org/10.48550/arXiv.2307.02612. 39

[66] Dalle Rocha, Lucas e Edna Dias Canedo: *Supplementary Material for Comparative Analysis of Data Protection Laws and Privacy Frameworks: Optimizing Solutions for Compliance with LGPD and International Data Sharing Laws*, maio 2024. https://doi.org/10.5281/zenodo.14037326. 42, 56, 112, 113, 125

[67] Pitogo, Vicente A. e Michelle Renee D. Ching: *Understanding philippine national agency's commitment on data privacy act of 2012: a case study perspective*. Em Ng, Vincent, Cheol Park, Young-Chang Hou, Kun-Huang Huarng e Alexander Wollenberg (editores): *Proceedings of the 2nd International Conference on E-commerce, E-Business and E-Government, ICEEG 2018, Hong Kong, SAR, China, June 13-15, 2018*, páginas 64–68. ACM, 2018. https://doi.org/10.1145/3234781.3234788. 42, 48, 49, 53

[68] Wong, Richmond Y., Andrew Chong e R. Cooper Aspegren: *Privacy legislation as business risks: How GDPR and CCPA are represented in technology companies' investment risk disclosures*. Proc. ACM Hum. Comput. Interact., 7(CSCW1):1–26, 2023. https://doi.org/10.1145/3579515. 42, 45, 46, 48

[69] 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. 42, 44, 45, 48, 53

[70] Daoudagh, Said e Eda Marchetti: *The GDPR compliance and access control systems: Challenges and research opportunities*. Em Mori, Paolo, Gabriele Lenzini e Steven Furnell (editores): *Proceedings of the 8th International Conference on Information Systems Security and Privacy, ICISSP 2022, Online Streaming, February 9-11, 2022*, páginas 571–578. SCITEPRESS, 2022. https://doi.org/10.5220/0010912300003120. 42, 45, 48, 50

[71] Weber, Philip Andreas, Nan Zhang e Haiming Wu: *A comparative analysis of personal data protection regulations between the EU and china*. Electron. Commer. Res., 20(3):565–587, 2020. https://doi.org/10.1007/s10660-020-09422-3. 42, 44

[72] Ayala-Rivera, Vanessa e Liliana Pasquale: *The grace period has ended: An approach to operationalize GDPR requirements*. Em Ruhe, Guenther, Walid Maalej e Daniel Amyot (editores): *26th IEEE International Requirements Engineering Conference, RE 2018, Banff, AB, Canada, August 20-24, 2018*, páginas 136–146. IEEE Computer Society, 2018. https://doi.org/10.1109/RE.2018.00023. 43, 46, 47, 48, 49

[73] Park, Grace: *The changing wind of data privacy law: A comparative study of the european union's general data protection regulation and the 2018 california consumer privacy act.* UC Irvine L. Rev., 10:1455, 2019. 43, 44, 45

[74] Pires, Filipe, Osvaldo R Pacheco e Ricardo T Martins: *Why you should care about gdpr in iot enterprises & solutions.* Em *2021 16th Iberian Conference on Information Systems and Technologies (CISTI)*, páginas 1–9. IEEE, 2021. 43, 48, 49

[75] Povse, Danaja Fabcic: *It's all fun and games, and some legalese: data protection implications for increasing cyber-skills of employees through games.* Em *Proceedings of the Central European Cybersecurity Conference 2018, CECC 2018, Ljubljana, Slovenia, November 15-16, 2018*, páginas 10:1–10:5. ACM, 2018. https://doi.org/10.1145/3277570.3277580. 43, 48

[76] Almeida, Denise R. S., Konstantin Shmarko e Elizabeth Lomas: *The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of us, eu, and UK regulatory frameworks.* AI Ethics, 2(3):377–387, 2022. https://doi.org/10.1007/s43681-021-00077-w. 43, 45

[77] Ribeiro, Renato Carauta e Edna Dias Canedo: *Using MCDA for selecting criteria of LGPD compliant personal data security.* Em Eom, Seok-Jin e Jooho Lee (editores): *dg.o '20: The 21st Annual International Conference on Digital Government Research, Seoul, Republic of Korea, June 15-19, 2020*, páginas 175–184. ACM, 2020. https://doi.org/10.1145/3396956.3398252. 43, 48

[78] Alhazmi, Abdulrahman e Nalin Asanka Gamagedara Arachchilage: *I'm all ears! Listening to software developers on putting GDPR principles into software development practice.* Pers. Ubiquitous Comput., 25(5):879–892, 2021. https://doi.org/10.1007/s00779-021-01544-1. 43, 48, 51, 52

[79] Kühtreiber, Patrick, Viktoriya Pak e Delphine Reinhardt: *A survey on solutions to support developers in privacy-preserving iot development.* Pervasive Mob. Comput., 85:101656, 2022. https://doi.org/10.1016/j.pmcj.2022.101656. 43, 48, 49

[80] Li, Ze Shi, Colin M. Werner, Neil A. Ernst e Daniela E. Damian: *GDPR compliance in the context of continuous integration.* CoRR, abs/2002.06830, 2020. https://arxiv.org/abs/2002.06830. 43, 48, 49, 50, 51, 53, 68, 69

[81] Serrado, João, Ruben Filipe Pereira, Miguel Mira da Silva e Isaías Scalabrin Bianchi: *Information security frameworks for assisting gdpr compliance in banking industry.* Digital Policy, Regulation and Governance, 22(3):227–244, 2020. 43, 48

[82] Aberkane, Abdel-Jaouad, Seppe vanden Broucke e Geert Poels: *Toward data protection by design: Assessing the current state of GDPR disclosure in web applications.* Em Schneider, Kurt, Fabiano Dalpiaz e Jennifer Horkoff (editores): *31st IEEE International Requirements Engineering Conference, RE 2023 - Workshops, Hannover, Germany, September 4-5, 2023*, páginas 218–223. IEEE, 2023. https://doi.org/10.1109/REW57809.2023.00044. 43, 48

[83] Canedo, Edna Dias, Vanessa Coelho Ribeiro, Ana Paula de Aguiar Alarcão, Lucas Alexandre Carvalho Chaves, Johann Nicholas Reed, Fábio Lúcio Lopes de Mendonça e Rafael Timóteo de Sousa Júnior: *Challenges regarding the compliance with the general data protection law by brazilian organizations: A survey.* Em Gervasi, Osvaldo, Beniamino Murgante, Sanjay Misra, Chiara Garau, Ivan Blecic, David Taniar, Bernady O. Apduhan, Ana Maria A. C. Rocha, Eufemia Tarantino e Carmelo Maria Torre (editores): *Computational Science and Its Applications - ICCSA 2021 - 21st International Conference, Cagliari, Italy, September 13-16, 2021, Proceedings, Part III*, volume 12951 de *Lecture Notes in Computer Science*, páginas 438–453. Springer, 2021. https://doi.org/10.1007/978-3-030-86970-0_31. 43, 44, 45, 48

[84] Poritskiy, Nazar, Flávio Oliveira e Fernando Almeida: *The benefits and challenges of general data protection regulation for the information technology sector.* Digital Policy, Regulation and Governance, 21(5):510–524, 2019. 43, 45, 48, 49, 51, 52

[85] Brodin, Martin: *A framework for gdpr compliance for small-and medium-sized enterprises.* European Journal for Security Research, 4:243–264, 2019. 43, 48, 49, 53

[86] Grundstrom, Casandra, Karin Väyrynen, Netta Iivari e Minna Isomursu: *Making sense of the general data protection regulation - four categories of personal data access challenges.* Em Bui, Tung (editor): *52nd Hawaii International Conference on System Sciences, HICSS 2019, Grand Wailea, Maui, Hawaii, USA, January 8-11, 2019*, páginas 1–10. ScholarSpace, 2019. https://hdl.handle.net/10125/59941. 43, 48, 50

[87] Ferrão, Sâmmara Éllen Renner, Artur Potiguara Carvalho, Edna Dias Canedo, Alana Paula Barbosa Mota, Pedro Henrique Teixeira Costa e Anderson Jefferson Cerqueira: *Diagnostic of data processing by brazilian organizations - A low compliance issue.* Inf., 12(4):168, 2021. https://doi.org/10.3390/info12040168. 43, 48, 49, 50, 65

[88] Horstmann, Stefan Albert, Samuel Domiks, Marco Gutfleisch, Mindy Tran, Yasemin Acar, Veelasha Moonsamy e Alena Naiakshina: *"those things are written by lawyers, and programmers are reading that." mapping the communication gap between software developers and privacy experts.* Proc. Priv. Enhancing Technol., 2024(1):151–170, 2024. https://doi.org/10.56553/popets-2024-0010. 43, 48, 49, 66

[89] Peixoto, Mariana Maia, Dayse Ferreira, Mateus Cavalcanti, Carla Silva, Jéssyka Vilela, João Araújo e Tony Gorschek: *On understanding how developers perceive and interpret privacy requirements research preview.* Em Madhavji, Nazim H., Liliana Pasquale, Alessio Ferrari e Stefania Gnesi (editores): *Requirements Engineering: Foundation for Software Quality - 26th International Working Conference, REFSQ 2020, Pisa, Italy, March 24-27, 2020, Proceedings [REFSQ 2020 was postponed]*, volume 12045 de *Lecture Notes in Computer Science*, páginas 116–123. Springer, 2020. https://doi.org/10.1007/978-3-030-44429-7_8. 43, 48, 50, 53, 73

[90] Tahaei, Mohammad, Alisa Frik e Kami Vaniea: *Privacy champions in software teams: Understanding their motivations, strategies, and challenges*. Em Kitamura, Yoshifumi, Aaron Quigley, Katherine Isbister, Takeo Igarashi, Pernille Bjørn e Steven Mark Drucker (editores): *CHI '21: CHI Conference on Human Factors in Computing Systems, Virtual Event / Yokohama, Japan, May 8-13, 2021*, páginas 693:1–693:15. ACM, 2021. https://doi.org/10.1145/3411764.3445768. 43, 48, 50, 51

[91] Freitas, M da C e Miguel Mira da Silva: *Gdpr compliance in smes: There is much to be done*. Journal of Information Systems Engineering & Management, 3(4):30, 2018. 43, 48, 49, 50, 52, 67, 71

[92] Shaheen, Yaqin, Miguel J Hornos e Carlos Rodríguez-Domínguez: *Iot security and privacy challenges from the developer perspective*. Em *International Symposium on Ambient Intelligence*, páginas 13–21. Springer, 2023. 43, 48

[93] Wiefling, Stephan, Jan Tolsdorf e Luigi Lo Iacono: *Data protection officers' perspectives on privacy challenges in digital ecosystems*. Em Katsikas, Sokratis K., Frédéric Cuppens, Christos Kalloniatis, John Mylopoulos, Frank Pallas, Jörg Pohle, M. Angela Sasse, Habtamu Abie, Silvio Ranise, Luca Verderame, Enrico Cambiaso, Jorge Maestre Vidal, Marco Antonio Sotelo Monge, Massimiliano Albanese, Basel Katt, Sandeep Pirbhulal e Ankur Shukla (editores): *Computer Security. ESORICS 2022 International Workshops - CyberICPS 2022, SECPRE 2022, SPOSE 2022, CPS4CIP 2022, CDT&SECOMANE 2022, EIS 2022, and SecAssure 2022, Copenhagen, Denmark, September 26-30, 2022, Revised Selected Papers*, volume 13785 de *Lecture Notes in Computer Science*, páginas 228–247. Springer, 2022. https://doi.org/10.1007/978-3-031-25460-4_13. 43, 48, 51, 68

[94] Buckley, Gerard, Tristan Caulfield e Ingolf Becker: *"it may be a pain in the backside but..." insights into the resilience of business after GDPR*. Em *Proceedings of the 2022 New Security Paradigms Workshop, NSPW 2022, North Conway, NH, USA, October 24-27, 2022*, páginas 21–34. ACM, 2022. https://doi.org/10.1145/3584318.3584320. 43, 48, 49, 51

[95] Teixeira, Gonçalo Almeida, Miguel Mira da Silva e Ruben Pereira: *The critical success factors of gdpr implementation: a systematic literature review*. Digital Policy, Regulation and Governance, 21(4):402–418, 2019. 43, 48, 49, 50, 66, 70

[96] Holler, Manuel, Benjamin van Giffen, Seth Benzell e Matthias Ehrat: *The general data protection regulation in financial services industries: how do companies approach the implementation of the gdpr and what can we learn from their approaches*. Proceedings of the 82th Jahrestagung des Verbands der Hochschullehrer für Betriebswirtschaft (VHB), páginas 1–11, 2020. 43, 48

[97] Hirvonen, Pauliina: *A review of GDPR impacts on information security*. Em Huang, Ming-Hui, Guy Gable, Christy M. K. Cheung e Dongming Xu (editores): *26th Pacific Asia Conference on Information Systems, PACIS 2022, Virtual Event / Taipei, Taiwan / Sydney, Australia, July 5-9, 2022*, página 83, 2022. https://aisel.aisnet.org/pacis2022/83. 43, 48, 50

[98] Ekambaranathan, Anirudh, Jun Zhao e Max Van Kleek: *"money makes the world go around": Identifying barriers to better privacy in children's apps from developers' perspectives*. Em Kitamura, Yoshifumi, Aaron Quigley, Katherine Isbister, Takeo Igarashi, Pernille Bjørn e Steven Mark Drucker (editores): *CHI '21: CHI Conference on Human Factors in Computing Systems, Virtual Event / Yokohama, Japan, May 8-13, 2021*, páginas 46:1–46:15. ACM, 2021. https://doi.org/10.1145/3411764.3445599. 43, 48, 50, 52

[99] Justice, State of California Department of: *California consumer privacy act*, 2018. https://cppa.ca.gov/regulations/pdf/cppa_act.pdf, acesso em 14/10/2023. 80, 82

[100] Davis, Fred D: *Perceived usefulness, perceived ease of use, and user acceptance of information technology*. MIS quarterly, páginas 319–340, 1989. 112

[101] Wohlin, Claes, Per Runeson, Martin Höst, Magnus C Ohlsson, Björn Regnell e Anders Wesslén: *Experimentation in software engineering*. Springer Science & Business Media, 2012. 122