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

Aplicação dos Princípios da Lei Geral de Proteção de Dados por Desenvolvedores de Software

Lucas Dalle Rocha
Matheus Breder Branquinho Nogueira

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

Orientadora
Prof.a Dr.a Edna Dias Canedo

Brasília
2022

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

Aplicação dos Princípios da Lei Geral de Proteção de Dados por Desenvolvedores de Software

Lucas Dalle Rocha
Matheus Breder Branquinho Nogueira

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

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

Prof.a Dr.a Fernanda Lima
CIC/UnB

Dr. Aleteia Patricia Favacho de Araujo
CIC/UnB

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

Brasília, 12 de setembro de 2022

Dedicatória

Dedicamos este trabalho primordialmente aos nossos pais, que sempre nos motivaram em nosso percurso acadêmico e na vida, a fim de que fôssemos a melhor versão de nós mesmos. Ademais, dedicamos aos amigos pessoais e da faculdade, que contribuíram com momentos descontraídos e de aprendizagem em grupo, respectivamente. Da mesma forma, dedicamos o trabalho aos nossos professores do curso, que nos proporcionaram um ambiente de aprendizado e de evolução pessoal.

Agradecimentos

Agradecemos especialmente aos nossos familiares e amigos próximos pelos incentivos e pela convivência que nos proporcionou uma esfera social favorecida em saúde mental. Aos professores e colegas do curso, agradecemos pela união e pelo auxílio em diversas matérias.

Resumo

Em um cenário de crescente utilização de aplicações digitais, violações de dados se tornam cotidianas. É importante que desenvolvedores e projetistas dessas tecnologias estejam em conformidade com normas que garantam a privacidade dos usuários, que no Brasil é prevista pela Lei Geral de Proteção de Dados Pessoais (LGPD). Assim, este trabalho tem como objetivo identificar os principais obstáculos que impedem os profissionais de software de garantir os princípios da LGPD em suas aplicações. Além disso, apresenta uma proposta de um guia referencial, a fim de auxiliar os profissionais de Tecnologia da Informação e Comunicação (ICT) em relação às suas respectivas dificuldades com a implementação de tais princípios. Para isso, realizou-se uma revisão de literatura para identificar trabalhos relacionados à privacidade, além de técnicas e *frameworks* utilizados na implementação de aplicações. Ademais, desenvolveu-se um cenário experimental que apresenta funcionalidades semelhantes as de aplicações *web*. Assim, conduziu-se um questionário com profissionais que atuam em diferentes áreas do desenvolvimento de software, a fim de averiguar a conformidade com a LGPD, baseada no conhecimento de técnicas que seriam utilizadas no cenário. Os resultados da pesquisa mostraram que todos os participantes apresentaram dificuldade em pelo menos um dos princípios da LGPD, de modo que a maioria foi pela falta de conhecimento de técnicas de implementação que garantam por completo a privacidade dos dados de usuários. Assim, é necessário que os profissionais de desenvolvimento de software aprimorem o aprendizado em relação às técnicas que garantam a privacidade e, semelhantemente, às diretrizes da LGPD.

Palavras-chave: Privacidade de Dados, Desenvolvedores de Software, Lei Geral de Proteção de Dados Pessoais, Requisitos de Privacidade

Abstract

With the increasing usage of digital applications, data breaches happen everyday. It is important that developers and designers of such technologies comply with standards that guarantee the privacy of users, which in Brazil it is provided by the General Personal Data Protection Law (LGPD). Thereby, this work aims to identify the main obstacles preventing software professionals from guaranteeing the principles of the LGPD in their applications. In addition, it presents a proposal of a reference guide, in order to help Information and Communication Technology (ICT) professionals regarding their respective difficulties with the implementation of such principles. Therefore, a literature review was carried out to elucidate papers related to privacy, as well as techniques and frameworks used in the implementation of applications. Furthermore, an experimental scenario was developed, that presents similar functionalities to web applications. Thus, a survey was conducted with professionals who work in different areas of software development, in order to verify compliance with the LGPD, based on the knowledge of techniques that would be used in the scenario. The survey results show that all participants had difficulty in at least one of the principles of the LGPD, most of them due to the lack of knowledge about implementation techniques that fully guarantee the privacy of user data. Thus, it is necessary that software development professionals improve their learning in relation to techniques that guarantee privacy and, similarly, to the guidelines of the LGPD.

Keywords: Data Privacy, Software Developers, General Personal Data Protection Law, Privacy Requirements

Sumário

Lista de Figuras

Lista de Tabelas

Capítulo 1

Introdução

Com o advento da Quarta Revolução Industrial e a formalização de conceitos cibernéticos relacionados, como *Big Data*, as aplicações e ferramentas digitais geram, diariamente, uma quantidade cada vez mais exorbitante de novos dados [1],[2]. Uma parcela majoritária da população mundial, isto é, aproximadamente 5 bilhões de pessoas, encontra-se ativamente conectada à Internet através da utilização de diversos dispositivos eletrônicos, sendo predominantemente, dispositivos móveis [3]. Em grande escala, isso se deve ao fato da popularização de plataformas sociais, que são fundamentadas no compartilhamento de diversos dados pessoais, desde nomes, fotos de perfil e até mesmo localizações de seus usuários [4]. Esse excessivo compartilhamento de dados coloca em pauta as questões de segurança de rede e de privacidade de dados pessoais no âmbito digital.

Por outro lado, segurança de rede trata-se de operações projetadas para garantir a confiabilidade e a integridade de quaisquer procedimentos em servidores, a título de exemplo, o armazenamento de dados em um banco de dados [5]. Não obstante, o tráfego de informações entre usuário e servidor — e vice-versa — denota a principal consideração de segurança de rede, no que consta à privacidade de dados pessoais, que deve ser abarcada pelos profissionais da área, tais como desenvolvedores e projetistas de software [5].

Na última década, o tratamento inadequado de dados pessoais ocasionou em diversas violações de dados, igualmente conhecidas como vazamentos de dados, por parte de renomadas empresas [6]. As operações irregulares de coleta, processamento, acesso, armazenamento e demais outras afetaram a autonomia individual de bilhões de usuários em casos recentes, como os das companhias LinkedIn [7], Yahoo [8], Twitter [9], Instagram [10] e, o mais polêmico, Facebook e Cambridge Analytica [11]. Dentre as informações que foram violadas acerca dos usuários estão: nome completo, endereço de *e-mail*, senha de acesso cifrado — *hash* —, preferências pessoais e até mesmo registros de geolocalização.

A privacidade de dados pessoais faz-se necessária pois quaisquer dados vazados, mesmo que generalizados, podem remeter a relação entre um indivíduo e suas individualidades,

como características pessoais e preferências [12]. O tratamento desses dados deve ser abarcado pelos desenvolvedores logo nas etapas iniciais do projeto, isto é, na etapas de concepção e elicitação de requisitos, a fim de reduzir potenciais conflitos entre segurança, confiabilidade e desempenho de um sistema [13].

A Lei Geral de Proteção de Dados (LGPD), denominada Lei n° 13.709, foi decretada no dia 14 de agosto de 2018 e substituiu o Marco Civil da Internet (Lei n° 12.965), ao passo que sanciona medidas que visam a proteção de dados pessoais [14],[15]. A lei define, no Art. 5°, o conceito de dado pessoal e dado pessoal sensível, este último crítico, uma vez que pode ocasionar discriminação em caso de vazamento. Ademais, a lei define políticas para tratamento de dados pessoais por parte dos responsáveis — denominado agentes de tratamento — no intuito de garantir o direito fundamental de privacidade e, caso contrário, acarreta sanções que serão aplicadas.

Nesse contexto, o desenvolvimento de software deve estar a par dos princípios protetivos implicados pela LGPD no Art. 6° [16],[14], uma vez que comporta uma série de normas que impedem a violação de dados pessoais, isto é, anulam a possibilidade de relação entre vazamento de dados pessoais críticos e titular dos dados. Assim sendo, os desenvolvedores devem conhecer em completude os princípios da LGPD e as organizações responsáveis devem verificar se o conceito de privacidade é respeitado em aplicações, de modo a auxiliar os profissionais com guias práticos e esclarecer problemas encontrados.

Diante deste cenário, faz-se necessária a contemplação de todos os princípios da LGPD por parte dos profissionais da área, de modo a garantir o direito de proteção legal de dados pessoais de quaisquer usuários, como consta no Art. 1°, *caput* da lei [14]. Dito isso, é importante quantificar e esquematizar os impasses expostos pelos desenvolvedores e projetistas de software, em um modelo de guia, que infligem diretamente a privacidade de um usuário titular durante a implementação de aplicações.

1.1 Problema de Pesquisa

Durante o desenvolvimento de aplicações, o tratamento de dados pessoais — sensíveis, inclusive — pode não receber a devida preocupação por parte dos profissionais envolvidos, o que resulta no uso indevido de tais dados e pode acarretar danos aos usuários [17]. Parte dos usuários não está ciente ou não se preocupa acerca dos seus direitos amparados pela Lei Geral de Proteção de Dados (LGPD) [18] e, por serem titulares, deveriam possuir um conhecimento e controle de todas as etapas de processamento de seus dados.

Uma parcela de desenvolvedores e projetistas de software demonstra não possuir familiaridade, ou entender os princípios de privacidade de software para garantir o tratamento adequado dos dados, ao passo que as organizações responsáveis ainda apresentam uma

certa dificuldade em elucidar as razões para o uso indevido dessas informações [19]. Não obstante, há carência de uma série de fatores por parte de organizações que implicam na quebra de privacidade, como a escassez de guias práticos direcionados e investimento monetário [17], e a falta de ferramentas específicas que auxiliem na etapa de desenvolvimento, com exemplificações dos fundamentos e princípios da LGPD [18]. Dessa forma, este trabalho investigará os problemas apontados pelos desenvolvedores de software durante a implementação de aplicações, no que diz respeito à garantia da privacidade dos usuários, de acordo com os princípios da LGPD.

1.2 Justificativa

A dicotomia entre a busca emergente por profissionais relacionados ao desenvolvimento de software e a falta de profissionais qualificados da área [20],[21] reflete a dificuldade em aplicar as leis cibernéticas vigentes do país, como a identificação adequada de requisitos de privacidade [13],[22]. Assim, a insuficiência de dados acerca dos problemas enfrentados pelos desenvolvedores e organizações contribui para que os princípios de leis vigentes de proteção de dados não sejam aplicados — ou aplicados incorretamente — e resulta em possibilidades de novos vazamentos de dados [17].

Este trabalho tem como meta identificar os principais pontos que carecem da atenção dos desenvolvedores de software, para que suas aplicações estejam em concordância com os artigos da Lei Geral de Proteção de Dados Pessoais (LGPD) [14] nas questões relacionadas à privacidade de dados. Não obstante, busca contribuir com informações relevantes acerca das dificuldades apontadas pelos desenvolvedores, a fim de que as organizações possam orientar seus desenvolvedores em pontos específicos e auxiliar quanto aos problemas elucidados.

1.3 Objetivos

1.3.1 Objetivo Geral

O objetivo deste trabalho é identificar os principais problemas relatados pelas equipes de desenvolvimento de software e pelos desenvolvedores de software, durante a etapa de desenvolvimento, quanto à implementação dos princípios da Lei Geral de Proteção de Dados (LGPD) para garantir a privacidade dos dados dos usuários nas aplicações de software.

1.3.2 Objetivos Específicos

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

1. Realizar uma contextualização em relação ao histórico de privacidade e das leis de proteção de dados, bem como do Regulamento Geral de Proteção de Dados — *General Data Protection Regulation (GDPR)* — e da Lei Geral de Proteção de dados (LGPD);
2. Relacionar a utilização de *frameworks* com a garantia da privacidade em aplicações de software, e sua influência na criação de leis jurídicas de proteção de dados pessoais;
3. Investigar as dificuldades e desafios dos membros das equipes de desenvolvimento de software, por meio de um *survey*, na aplicação dos princípios da LGPD;
4. Analisar se há conformidade dos profissionais no que diz respeito as diretrizes propostas pela LGPD;
5. Disponibilizar o resultado estatístico do *survey* e propor um guia referencial prático para elucidar as principais dificuldades dos profissionais.

1.4 Resultados Esperados

Ao final do trabalho espera-se alcançar, em completude, a disponibilização de um guia referencial para contribuir com a resolução dos principais problemas que interferem na aplicação dos princípios contidos na Lei Geral de Proteção de Dados (LGPD) relatados pelos desenvolvedores durante a realização de projetos de software.

1.5 Metodologia de Pesquisa

A metodologia adotada na condução do trabalho é o método experimental, que visa elaborar um ambiente de aplicação dos princípios da LGPD a fim de verificar como os objetos de estudo (desenvolvedores) se comportam. Além disso, este trabalho usa também o método monográfico, de modo a abarcar as influências do tema de maneira aprofundada e em amplitude [23]. Utiliza-se da pesquisa exploratória e descritiva, que integra o levantamento bibliográfico nos parâmetros da privacidade e suas leis de proteção de dados, e a utilização do procedimento de *survey* para coleta de informações acerca da aplicação dos princípios da LGPD por parte dos desenvolvedores. Acerca da análise dos questionários

é utilizada uma abordagem qualitativa, a fim de inferir os problemas relacionados à privacidade de dados apontados pelos desenvolvedores de software. As etapas adotadas no processo de metodologia de pesquisa deste trabalho são:

1. Revisão da ideia preliminar de privacidade;
2. Revisão de leis de privacidade históricas e vigentes (GDPR e LGPD);
3. Investigação e relação de trabalhos correlatos;
4. Questionamento acerca da aplicação dos princípios da LGPD por desenvolvedores de software;
5. Aplicação de um questionário para avaliar as adversidades relatadas pelos desenvolvedores;
6. Análise dos resultados dos questionários;
7. Proposição de um guia referencial para contribuição da conformidade em relação às diretrizes da LGPD;
8. Discussão acerca dos resultados e conclusão.

1.6 Estrutura do Trabalho Final de Curso

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 dos conceitos e das aplicações de privacidade, bem como os princípios, os requisitos de privacidade no contexto de software, e as leis de proteção de dados, sendo as de destaque o Regulamento Geral de Proteção de Dados e a Lei Geral de Proteção de Dados.

O Capítulo 3 aborda em alto nível de detalhe o processo de experimentação adotado e, além disso, o processo de elaboração e divulgação do *survey*. Assim, há abordagem das ferramentas utilizadas, da contextualização do cenário, dos procedimentos, das práticas adotadas para a elucidação dos resultados e do processo de desenvolvimento dos questionários.

O Capítulo 4 expõe dados a respeito dos obstáculos relatados pelos profissionais, haja vista a implementação dos princípios da LGPD. Além disso, há contemplação das situações de carência de conformidade dos profissionais em relação às diretrizes, com o intuito da proposição de um guia referencial prático de contribuição.

O Capítulo 5 apresenta a contribuição do trabalho no âmbito de desenvolvimento, por meio de uma síntese de todo o processo adotado neste trabalho. Ademais, o capítulo

aborda motivações para trabalhos posteriores, a fim de que sejam contempladas em novos objetos de estudo.

Capítulo 2

Referencial Teórico

Neste capítulo serão apresentados todos os conceitos relevantes para este trabalho e o referencial teórico para embasar a pesquisa.

2.1 Privacidade e Proteção de Dados

Inicialmente, é necessário entender as relações de privacidade para compreender o estudo que será feito. O direito à privacidade foi abordado juridicamente, pela primeira vez, em 1890 pela lei de privacidade norte-americana e é conceituado como o "direito de ser deixado só" [24]. Posteriormente, em 1948, foi garantido pela Organização das Nações Unidas (ONU) como um direito humano fundamental e universal [25]. No Brasil, a privacidade — dada como intimidade e vida privada — é garantida por lei como direito fundamental, haja vista o Art. 5°, inciso X da Constituição Federal de 1988 [26] e a inviolabilidade da vida privada de uma pessoa natural é declarada no Art. 21° do Código Civil de 2002 [27].

A conceitualização da privacidade em seus diferentes âmbitos pode ser dada através da separação de seus estágios de atuação no cotidiano. Westin et al. [28] afirmaram que existem quatro estados de privacidade que podem ser alcançados em um regime democrático, cada qual com suas particularidades do indivíduo e suas influências sociais, tanto exercidas quanto sofridas. A Tabela 2.1 apresenta a definição e exemplificação dos estados de privacidade descritos por Westin et al. [28].

Tabela 2.1: Estados de privacidade [28].

Estado	Descrição
Solitude	Estado em que há desagregação do indivíduo de seu grupo social e deixa de ser observável por esse último. Trata-se do estado mais completo de privacidade que pode ser alcançado.
Intimidade	Estado em que há isolamento do indivíduo em conjunto de outros pertencentes ao seu vínculo social mais íntimo, a título de exemplo família, amigos, colegas de trabalho, etc.
Anonimato	Estado em que há liberdade por parte do indivíduo de transitar em lugares públicos e, ainda assim, encontra-se livre de ser identificado e vigiado por outras pessoas, de modo a permanecer relaxado. Além disso, pode existir o desejo do indivíduo de compartilhar suas ideias de maneira anônima, isto é, sem que seja identificado como autor.
Reservação	Estado em que há restrição da comunicação por parte do indivíduo em resposta a uma intromissão indesejada. Trata-se do estado mais sutil de privacidade que pode ser alcançado.

Apesar da relevância de se definir o conceito de privacidade e suas aplicações no cotidiano, é necessário uma maior complementação do tema para o contexto digital, uma vez que a privacidade de um indivíduo se estende à privacidade de seus dados, isto é, informações que dizem respeito ao indivíduo [29]. Dessa forma, o "direito de ser deixado só" e seus estados impactantes (Tabela 2.1) tiveram de ser aprimorados para garantir a integralidade da privacidade de um indivíduo em uma sociedade cada vez mais tecnológica.

Diz-se a respeito da privacidade de dados de um indivíduo a consideração de qualquer operação realizada sobre esses dados — posteriormente apresentados na Figura 2.3 — por um terceiro, seja eles produzidos pelo próprio indivíduo ou por seu responsável, dado o aval [19]. Em consequência da extensão do conceito de privacidade no meio digital, fez-se necessária a adequação de normas referentes a aplicações em base de dados, a fim de se evitar violações que não eram factíveis previamente.

Historicamente, de acordo com Mayer-Schönberger [30], as leis de proteção de dados pessoais podem ser atribuídas a quatro gerações. A primeira geração marca o início da década de 1970 em que o acesso tecnológico demandava alto capital, ou seja, apenas uma seleta parte da população dispunha de tal. As leis eram direcionadas em completude ao Estado, uma vez que esse era responsável pela criação e administração de grandes centros de dados, de modo que cidadão algum detinha conhecimento acerca dos procedimentos utilizados para tratamento de seus dados. Ademais, pelo receio de limitação do crescimento tecnológico por parte de leis de controle do tratamento de dados, essas últimas eram brandas e decretavam instâncias relativas aos centros de dados, mas não diretamente à privacidade. Embora essas normas apresentassem certa regulamentação acerca do tratamento de dados, o crescimento contínuo de centros de processamento não cooperava com a centralização desejada pelo Estado, e houve necessidade de uma reforma jurídica [31].

A segunda geração, por sua vez, teve base no final de década de 1970. A responsabilidade de controle do tratamento de dados pessoais foi atribuída aos cidadãos e o Estado passou a funcionar como um facilitador de informações. O diferencial dessa geração é que o dever do Estado era informar os cidadãos acerca da utilização de seus dados, e cabia ao cidadão comprovar a finalidade e possuía a liberdade de alertar em caso de uso indevido. A necessidade da ativa participação do cidadão para manutenção da privacidade de seus dados foi um problema e, ademais, se reflete até os dias atuais, em que parte da população não se interessa pelos riscos da exposição indevida de suas informações pessoais [18]. Assim como no início da década, foi inevitável um reparo nas normas dispostas dessa geração [31].

A terceira geração teve início na década de 1980 e a principal aplicação foi o reforço da liberdade de escolha do cidadão sobre o tratamento de seus dados pelo conceito de autodeterminação informativa. Dado que o tratamento de dados dispõe de múltiplas operações, passou-se a integralizar os cidadãos em todas as etapas possíveis de operações, a fim de que a liberdade estimada na segunda geração pudesse ser alcançada. Embora as leis de proteção tenham se assemelhado às atuais, o mesmo impasse observado na geração anterior foi sinalizado e apenas uma parcela da população usufruía de tais direitos [31].

Por fim, a quarta geração engloba o período da década de 1990 até a atualidade. A motivação dessa geração foi solucionar os obstáculos dispostos pelas últimas gerações (especificamente as últimas duas) em obter um equilíbrio entre a vontade individual e o bem coletivo. Desse modo, buscou-se atribuir leis específicas para cada setor de atuação, a fim de se evitar o impacto negativo do tratamento de dados dada a especificidade de cada área [31]. No Brasil, a lei vigente é a Lei Geral de Proteção de Dados Pessoais (LGPD), que tem como base a lei europeia *General Data Protection Regulation* (GDPR) e ambas leis são apresentadas na Seção 2.2. Os principais pontos decorrentes de cada geração podem ser observados na Figura 2.1.

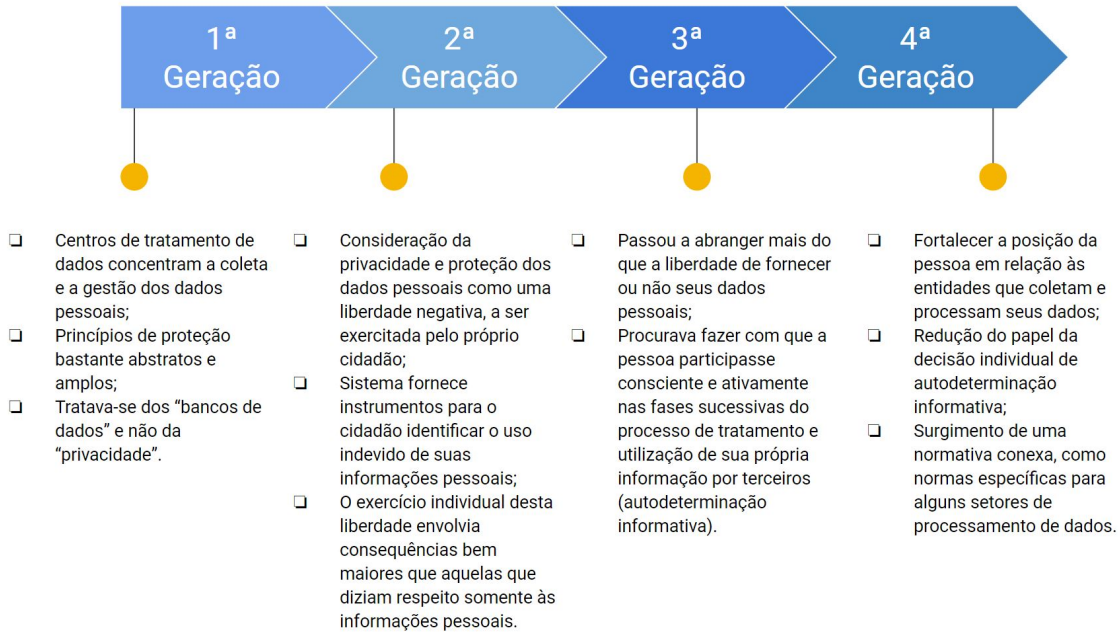

Figura 2.1: Particularidades de cada geração das leis de proteção de dados [31].

2.1.1 Princípios e Limitações da Privacidade

Os Princípios de Práticas de Informações Justas — proposto em *The Code of Fair Information Practices* —, elaborados inicialmente em 1973 pelo Departamento de Saúde, Educação e Bem-Estar dos Estados Unidos da América, apresentam uma série de recomendações com o intuito de resguardar o direito da proteção de dados pessoais dos cidadãos norte-americanos. Dessa forma, correspondem à base da elaboração de normas que relacionam privacidade e dados pessoais, e são apresentados como os seguinte cinco princípios básicos [32]:

1. Não deve haver um sistema de armazenamento de dados pessoais o qual sua existência seja mantida em segredo;
2. Deve haver uma maneira de um indivíduo apurar quais informações sobre ele estão sendo mantidas em registro e como elas são utilizadas;
3. Deve haver uma maneira de um indivíduo prevenir que a sua informação previamente coletada para um propósito estipulado seja utilizada (ou disponibilizada) para algum outro propósito, sem o seu consentimento;
4. Deve haver uma maneira de um indivíduo corrigir ou alterar um registro de informação sobre si;

5. Qualquer organização que crie, mantenha, utilize ou dissemine registros com dados pessoais deve garantir a confiabilidade dos dados para a finalidade pretendida e deve tomar precauções para prevenir o uso indevido dos mesmos.

Embora a exposição desses fundamentos estivesse meramente em um estágio inicial, no que tange a proteção de dados pessoais estabelecida atualmente, é possível enumerar e conceituar tais princípios supracitados, como: "Princípio da publicidade", "Princípio da exatidão", "Princípio da finalidade", "Princípio do livre acesso" e "Princípio da segurança", respectivamente. [31].

O alicerce para a elaboração de renomadas leis de proteção de dados vigentes — como GDPR e LGPD —, foi a proposta de oito princípios, em 1980, estabelecidos pelas diretrizes da Organização para a Cooperação e Desenvolvimento Econômico (OCDE) para a proteção de privacidade e fluxo de dados pessoais [33]. É importante ressaltar que essas diretrizes foram influenciadas, em abrangência, pelos Princípios de Práticas de Informações Justas propostos em 1973. A relevância dessas diretrizes é irrevogável, uma vez que os princípios — atualizados em 2013 — apresentam-se integralmente idênticos aos sugeridos em 1980 e, ademais, é indispensável sua influência no desenvolvimento de normas nacionais e internacionais acerca da proteção de dados. Os oito princípios são apresentados a seguir, bem como suas descrições [33]:

1. Princípio da Coleta Limitada: deve haver limites para a coleta de dados pessoais e esses dados devem ser obtidos de maneira justa e legal e, quando conveniente, com a compreensão e consentimento do titular dos mesmos;

2. Princípio da Qualidade de Dados: os dados pessoais devem ser importantes para os fins que são utilizados e, na medida do possível — em relação aos propósitos —, devem ser precisos, completos e mantidos atualizados;

3. Princípio da Especificação de Finalidade: a finalidade pelos quais os dados pessoais são coletados deve ser especificada tão antes quanto da coleta dos dados e a utilização posterior deve ser limitada para a satisfação da finalidade ou outra que não seja incompatível com a finalidade inicial, e seja especificada em cada caso de alteração da finalidade;

4. Princípio da Limitação do Uso: os dados pessoais não devem ser divulgados, disponibilizados ou utilizados para propósitos diferentes dos especificados no Princípio da Especificação de Finalidade, exceto: a) em caso de permissão do indivíduo; ou b) por autoridade jurídica;

5. Princípio das Proteções de Segurança: os dados pessoais devem ser protegidos por moderadas proteções de segurança contra riscos como perda ou acesso não autorizado, destruição, utilização, modificação ou divulgação dos dados;

6. Princípio de Abertura: deve haver uma política geral de abertura sobre desenvolvimentos, práticas e políticas em respeito aos dados pessoais. Recursos devem ser facilmente disponibilizados para estabelecer a existência e a natureza dos dados, e a finalidade principal para a sua utilização, bem como a identificação e localidade do controlador dos dados;

7. Princípio da Participação Individual: um indivíduo deve ter o direito: a) de obter de um controlador de dados a confirmação de que o controlador possui ou não dados que se referem ao indivíduo; b) de ser comunicado acerca de dados referentes a si

   - em tempo razoável;
   - a um custo, se houver, que não seja excessivo;
   - de uma maneira razoável; e
   - de uma forma que seja facilmente compreensível por ele;

   c) de receber as razões caso as requisições feitas sobre os subparágrafos (a) e (b) sejam negadas, e de ser apto a contestar tais negações; e d) de contestar dados referentes a si e, caso obtenha sucesso na contestação de ter os dados apagados, retificados, concluídos ou alterados;

8. Princípio da Responsabilidade: o controlador dos dados deve ser responsável por tomar as medidas necessárias para fazer valer os princípios citados anteriormente.

Apesar das análises e discussões realizadas acerca da privacidade de dados, essa última ainda não abrange todos os âmbitos sociais. O rápido avanço do desenvolvimento da tecnologia também traz riscos à privacidade, como o desenvolvimento de tecnologias de invasão de privacidade (*Privacy-Invading Technologies*) [34]. Além disso, o próprio conceito de privacidade por *design* ainda necessita de melhores ferramentas para avaliar os padrões de privacidade e sua garantia de qualidade nos sistemas de software [35].

Os esforços para alcançar a privacidade de dados são intensos. Além disso, uma parte importante nessa análise é o fator desempenho dos sistemas de software ao aplicar os mecanismos de privacidade de dados. Ao adotar os princípios de privacidade no projeto de software, sempre haverá uma troca — *trade-off* — entre desempenho e privacidade [36]. Visto que os problemas de vazamento de dados privados são frequentes e tem efeitos negativos diversos numa sociedade altamente tecnológica, é válido o investimento em garantir a privacidade dos dados de indivíduos, mesmo que cause um desempenho inferior dos sistemas de software.

2.1.2 Requisitos de Privacidade no Desenvolvimento de Software

Desde a formulação do conceito de privacidade e das primeiras normas para se assegurar a proteção de dados pessoais, viu-se a importância da instituição de princípios a serem cumpridos, tanto pelo usuário quanto pelo responsável jurídico. No contexto de desenvolvimento de software não foi diferente, visto que a salvaguarda da privacidade e a proteção de dados estão intimamente ligadas a preservação dos mesmos, de modo que não ocorra a violação dos dados pessoais, conhecida pelo termo *data breach* [17],[6].

Previamente aos regulamentos sobre proteção de dados pessoais, os *frameworks*, que postulam fundamentos de privacidade direcionados à implementação de serviços digitais, funcionavam como embasamento primário para desenvolvedores e projetistas de software [37]. Esse é o cenário do conceito *Privacy by Design* (PbD), criado em 1995 em relatório canadense denominado *Privacy-enhancing technologies* [38]. O PbD busca estender os princípios básicos — Princípios de Práticas de Informações Justas — apresentados na Seção 2.1.1 no contexto de Engenharia de Software, ou seja, há enfoque na aplicação das práticas de proteção de dados por desenvolvedores da área de tecnologia. Desse modo, é imprescindível compreender os princípios propostos pelo PbD, haja vista a essência desse conceito presente na lei vigente europeia GDPR e, posteriormente, na lei vigente brasileira LGPD. Segue a especificação e a descrição em tópicos de sete princípios fundacionais do PbD, propostos por Ann Cavoukian [39]:

1. *Proativo não Reativo; Preventivo não Remediativo*

    - Essa abordagem do PbD é caracterizada por tomar medidas proativas ao invés de reativas. Há interesse em antecipar eventos de invasão de privacidade antes mesmo que ocorram, isto é, não deve haver uma espera de que riscos de privacidade aconteçam, nem deve oferecer uma correção para resolver uma infração de privacidade em suposição que ocorra. O propósito é prevenir em completude que uma infração ocorra.
    - O PbD expõe um reconhecimento explícito do valor e do benefício de se adotar medidas de privacidade em tecnologia de informação, de modo antecipado e consistente. As implicações disso são: o alto comprometimento de implantar um padrão elevado de privacidade, geralmente maior que os declarados por leis e regulamentações globais; o comprometimento com privacidade que é compartilhado por comunidades e *stakeholders*, dada a cultura de melhoria contínua; e o estabelecimento de métodos para reconhecer designs, práticas e resultados frágeis, no quesito privacidade, a fim de corrigir impactos negativos.

2. *Privacidade como Configuração Padrão*

- O PbD procura entregar o maior grau de privacidade ao garantir que dados pessoais serão automaticamente protegidos em qualquer sistema de tecnologia de informação ou prática de negócios. Mesmo que um indivíduo não faça nada, seus dados permanecem intactos, ou seja, nenhuma ação é necessária ao usuário para garantir a privacidade de seus dados.
- Esse princípio do PbD, também conhecido como *Privacy by Default*, aplica as seguintes medidas de fundamentos de informação justa, vide Tabela 2.2:

Tabela 2.2: Fundamentos do *Privacy by Default* [39].

Princípio do *Privacy by Default*	**Descrição**	**Princípio equivalente proposto pela OCDE**
Especificação do Propósito	O propósito pelo qual a informação de um usuário é coletada, utilizada, retida e divulgada deve ser comunicado ao usuário antes da coleta dessa informação. Propósitos específicos devem ser compreensíveis, limitados e relevantes para a situação em que os dados do usuário serão utilizados.	Princípio da Especificação da Finalidade [33]
Limitação da Coleta	A coleta de informações pessoais deve ser justa, legal e limitada aos fins especificados.	Princípio da Coleta Limitada [33]
Minimização de Dados	A coleta de dados pessoais deve ser mínima. O design de programas, sistemas, tecnologias de informação e comunicação devem começar, por padrão, com interações e transações não identificáveis. Sempre que for possível, os aspectos de identificação, de observação e de conexão de informações pessoais deve ser minimizado.	Ausente
Limitação de Uso, Retenção e Divulgação	O uso, retenção e divulgação de informações pessoais deve ser limitada aos propósitos relevantes ao indivíduo, o qual deu o consentimento, exceto em caso requerido por lei. Informações pessoais devem ser retidas apenas enquanto forem necessárias para satisfazer os propósitos declarados, e então seguramente eliminadas.	Propósito da Limitação do Uso [33]

3. *Privacidade Embutida no Design*

- O PbD é embutido no *design* e na arquitetura dos sistemas de tecnologia da informação. Uma abordagem sistemática e baseada em princípios deve ser adotada para embutir a privacidade – uma que possua padrões aceitáveis (frameworks) e seja receptiva às avaliações externas. Assim, a privacidade se torna um componente essencial para as funcionalidades do sistema, sem que elas sejam afetadas.
- Sempre que possível, impactos relacionados à privacidade e avaliações de risco devem ser feitos e publicados, em conjunto a uma documentação clara acerca dos riscos e as medidas tomadas para mitigar tais riscos.

- Os impactos de privacidade da tecnologia resultante e seus usos devem ser mínimos, além de não ser facilmente degradável com uso, erro ou configuração incorreta.

4. *Funcionalidade Completa - Soma-Positiva, não Soma-Zero*

   - O PbD almeja conciliar todos os interesses e objetivos de uma maneira "ganha-ganha", não apenas avaliar qual a melhor troca entre privacidade e funcionalidade. O PbD evita falsas dicotomias, como "privacidade *vs.* segurança", de modo a demonstrar ser possível obter ambas.
   - Ademais, almeja não apenas evitar empecilhos para as funcionalidades do sistema, mas otimizar tais requerimentos, a fim de se obter uma funcionalidade total do sistema.
   - Todos os interesses e objetivos devem ser claramente documentados, funcionalidades desejadas articuladas, métricas aceitas e implementadas, e rejeita a ideia de ter que escolher a privacidade em detrimento da funcionalidade — e vice-versa —, de modo a buscar a multifuncionalidade.

5. *Segurança de Ponta-a-Ponta - Proteção durante todo o Ciclo de Vida*

   - O PbD busca ampliar a segurança do dado durante todo o seu ciclo de vida na aplicação em que é utilizado. Esse princípio garante que a informação é mantida segura durante todo o processo, desde que é coletada até ser eliminada.
   - Não deve haver brechas de proteção, nem de responsabilidade. O princípio apresenta uma relevância especial, dado que sem uma segurança robusta, não tem como haver privacidade.
   - Entidades devem assumir a responsabilidade pela segurança da informação pessoal durante todo o ciclo de vida dos dados. Além disso, padrões de segurança — como métodos de eliminação segura, criptografia apropriada e controle de acesso consistente — devem garantir a confidencialidade, integridade e disponibilidade por todo o ciclo de vida dos dados pessoais.

6. *Visibilidade e Transparência - Mantê-lo Aberto*

   - O PbD propõe garantir aos *stakeholders* que, independente da tecnologia envolvida, ela opere de acordo com as premissas e objetivos estabelecidos, de modo que esteja sujeita a verificação. Os componentes e as operações são mantidos visíveis e transparentes, tanto aos usuários quanto aos provedores.

- Apesar do princípio dizer respeito a todas as Práticas de Informações Justas, é essencial ressaltar as seguintes medidas apresentadas a seguir, que se relacionam com o Princípio de Abertura proposto pela OCDE [33], na Tabela 2.3:

Tabela 2.3: Práticas de Visibilidade e Transparência [39].

Prática de Visibilidade e Transparência	**Descrição**
Prestação de Contas ou Responsabilidade	A coleta de informações pessoais implica no dever de cautela para tal proteção. A responsabilidade de quaisquer política e procedimentos relacionados à privacidade deve ser documentada e comunicada apropriadamente, e atribuída ao indivíduo. Ao transferir informações pessoais a terceiros, a proteção de privacidade deve ser assegurada de maneira equivalente.
Abertura	A abertura e a transparência são essenciais para a prestação de contas. Informações acerca das práticas e políticas de gerenciamento de informações pessoais devem estar prontamente disponibilizadas aos usuários.
Submissão	Submissão e mecanismos de reparo devem ser criados e as suas informações devem ser comunicadas aos usuários. Formas de monitorar, avaliar e verificar a submissão com práticas e procedimentos de privacidade também devem ser disponibilizadas.

7. *Respeito pela Privacidade do Usuário - Mantê-lo Centrado no Usuário*

- Os operadores e arquitetos dos sistemas devem manter os interesses do indivíduo de maneira predominante, de modo a oferecer medidas robustas de segurança, notificações apropriadas e alternativas amigáveis aos usuários. O melhor PbD é aquele que é projetado, de maneira consciente, em cima dos interesses e necessidades dos usuários.
- O respeito pela privacidade do usuário é garantido pela submissão, referente a Tabela 2.3, e pelas seguintes medidas adicionais, dada a Tabela 2.4:

Tabela 2.4: Práticas de Respeito à Privacidade do Usuário [39].

Práticas de Respeito à Privacidade	**Descrição**
Consentimento	O consentimento espontâneo e específico do indivíduo é obrigatório para a coleta, utilização ou divulgação de informações pessoais, exceto em casos amparados pela lei. Quanto maior a sensibilidade dos dados, mais evidente e específico deve ser o consentimento necessário. Ademais, o consentimento pode ser retirado, posteriormente.
Precisão	Informações pessoais devem ser precisas, completas e atualizadas, uma vez que são necessárias para satisfazer os propósitos especificados.
Acesso	Aos indivíduos deve ser proporcionado acesso as suas informações pessoais e devem ser informados acerca da utilização e divulgação. Além disso, os indivíduos devem estar aptos a contestar a precisão e completude das informações, e tê-las alteradas apropriadamente.

Caso os requisitos de privacidade forem identificados durante a fase inicial do desenvolvimento de software, é possível prevenir violações de privacidade. Tais requisitos de

privacidade devem ser especificados nas fases de concepção ou elicitação de um projeto de software. Além disso, durante todo o processo de desenvolvimento do software, os princípios de privacidade devem ser levados em conta, seja como requisitos funcionais ou não funcionais [40].

Em síntese, *frameworks* como o PbD reforçam a necessidade de que os desenvolvedores de software estabeleçam os requisitos de privacidade quanto antes da implementação [41]. Ainda mais recente, o Instituto Nacional de Padrões e Tecnologia publicou, em janeiro de 2020, uma ferramenta — NIST *Privacy Framework* — para auxiliar organizações na identificação de riscos de privacidade, estratégias para evitar vazamento de dados e o controle requerido para o tratamento de dados por todo o ciclo de vida [42]. A Figura 2.2 ilustra o fluxo desde o surgimento do problema na etapa de processamento de dados até os impactos prejudiciais às organizações responsáveis:

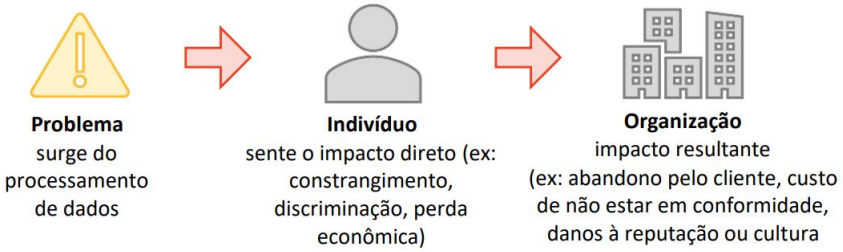

Figura 2.2: Fluxo de risco de privacidade [42].

Tem-se, portanto, a magnitude de se assegurar que as normas de proteção de dados sejam respeitadas e utilizadas por desenvolvedores e, em consequência disso, deve-se averiguar os obstáculos encontrados pelos mesmos no processo da garantia dos requisitos de privacidade [17]. De outro modo, a antiética por parte de organizações no tratamento de dados e, dessa forma, a iminente violação de informações motiva não somente a perda monetária dessas organizações, mas também a redução de usuários e confiança dos mesmos, a título de exemplo, o resultado do escândalo da empresa Facebook e a empresa de mineração de dados Cambridge Analytica [43].

Destarte, através da contextualização dos conceitos de privacidade e proteção de dados pessoais no âmbito digital e o papel do desenvolvedor em respaldar a aplicação das mesmas [17], há fundamento para tratar duas indispensáveis leis vigentes que defendem a integridade das informações pessoais atualmente: a GDPR e a LGPD.

2.2 Regulamentações da Privacidade e Tratamento de Dados

2.2.1 Regulamento Geral sobre a Proteção de Dados

O Regulamento Geral sobre a Proteção de Dados — *General Data Protection Regulation* (GDPR) — assinado em 14 de abril de 2016 pelo Parlamento Europeu e Conselho da União Europeia permanece em vigor desde 25 de maio de 2018 [44]. O GDPR surge pela necessidade de evitar a crescente violação de dados pessoais na era digital, dada a abrupta mudança no contexto de privacidade [45]. Além disso, o regulamento fundamenta uma série de normas que visa a proteção de dados dos cidadãos residentes da União Europeia (UE), a fim de evitar tais violações de dados [6]. Não obstante, o GDPR não se limita apenas ao processamento dos dados em território da UE, mas se aplica a qualquer atividade referente aos dados pessoais desde que pertençam aos cidadãos residentes, independente do país de origem em que são tratados, com aplicação de sanções administrativas em caso de violações [46]. Desse modo, o primeiro parágrafo do Artigo 1 do GDPR [44] pleiteia que o regulamento:

> "estabelece regras relativas à proteção das pessoas naturais no que diz respeito ao tratamento de dados pessoais e regras relativas à livre circulação de dados pessoais."

Para alcançar a unificação do tratamento de dados pessoais com o intuito de fortalecer o mercado digital europeu [46], o GDPR postula no Artigo 6 os termos para legalidade referentes ao processamento dos dados. Desses, o primeiro é dado por um tratamento prescindível e todos os outros termos são tratamentos necessários, dadas as circunstâncias [44]:

1. O tratamento está em sua legalidade se pelo menos um dos termos seguintes se aplica:
   (a) o titular concedeu permissão para o tratamento dos seus dados pessoais para um ou mais respectivos fins;
   (b) o processamento é necessário para a execução do contrato pelo qual o titular está inserido ou como medida necessária para que o titular faça parte do contrato;
   (c) o processamento é necessário para estar em conformidade com a obrigação legal ao qual o controlador está sujeito;
   (d) o processamento é necessário para proteger os interesses vitais do titular ou de outra pessoa natural;

(e) o processamento é necessário para a execução de uma tarefa referente a interesses públicos ou referente à autoridade oficial;

(f) o processamento é necessário para os fins de legítimo interesse pelo controlador ou terceiros, exceto caso os interesses sejam sobrescritos pelos interesses ou direitos fundamentais e liberdade do titular que requer a proteção dos dados pessoais (em particular caso em que o titular faz parte da menoridade).

Ademais, é importante compreender a terminologia utilizada no regulamento. O Artigo 4 do GDPR dispõe as definições que são relevantes no contexto do processamento de dados pessoais [44]:

- Titular dos dados: pessoa natural identificada ou identificável a partir de seus dados pessoais; uma pessoa natural identificável é um indivíduo que pode ser identificado pelos seus dados como, a título de exemplo, nome, número da identificação, localização geográfica e, mais geral, dados físicos, psicológicos, genéticos, mentais, econômicos, culturais ou sociais;
- Dados pessoais: qualquer informação acerca do titular (identificável);
- Processamento: quaisquer operações — ou conjunto de operações — realizadas em dados pessoais — ou conjunto de dados pessoais —, sejam automatizadas ou não, como coleção, gravação, organização, estruturação, armazenamento, adaptação ou alteração, recuperação, consulta, utilização, divulgação por transmissão, disseminação ou disponibilização, alinhamento ou combinação, restrição, eliminação ou destruição;
- Perfilamento: qualquer modo de processamento automatizado de dados pessoais que consiste na utilização dos dados pessoais para estimar características que dizem respeito ao desempenho da pessoa natural no trabalho, situação econômica, saúde, preferências pessoais, interesses, confiança, comportamento, localização ou movimentações;
- Pseudonimização: o processamento de dados pessoais de uma maneira que os mesmos não podem mais ser atribuídos ao titular específico (não mais identificável);
- Controlador: pessoa natural ou legal, autoridade pública, agência ou outra corporação que, isolada ou em conjunto com outros, determina os fins e medidas para o processamento dos dados pessoais;
- Processador: o atuante possui as mesmas características do controlador, exceto sua responsabilidade, que é o processamento de dados pessoais exigido pelo controlador.

No Artigo 5 do GDPR há a estipulação de sete princípios relacionados ao processamento de dados pessoais, de modo que são divididos em duas seções: a primeira abriga seis princípios que são relacionados diretamente à manipulação de dados pessoais; e a segunda contém um único princípio que diz respeito ao controlador. Com intuito de resguardar a privacidade de dados dos usuários europeus, segue a descrição dos princípios separados em seções e suas respectivas designações [44]:

1. Dados pessoais devem ser:

   (a) processados de maneira legal, justa e transparente em referência ao titular (Princípio da Legalidade, Justiça e Transparência);

   (b) coletados para fins específicos, explícitos e legítimos e não ser processados de maneira incompatível aos fins especificados (Princípio da Limitação de Propósito);

   (c) adequados, importantes e limitados ao que é necessário em relação aos fins pelos quais eles são processados (Princípio da Minimização de Dados);

   (d) precisos e, quando necessário, atualizados; toda medida sensata deve ser tomada para assegurar que os dados pessoais que são imprecisos, considerando os fins para que são processados, sejam apagados ou alterados sem atraso (Princípio da Precisão);

   (e) guardados de um modo que permite a identificação do titular dos dados apenas enquanto necessário aos fins para que os dados são processados (Princípio da Limitação de Armazenamento);

   (f) processados de modo que assegura a segurança apropriada dos dados pessoais, incluindo proteção contra processamento não autorizado ou ilegal e contra perda acidental, destruição ou danificação, utilizando técnicas ou medidas organizacionais apropriadas (Princípio da Integridade e Confidencialidade).

2. O controlador deve ser responsável e ser capaz de demonstrar conformidade por todos os princípios anteriormente citados (Princípio da Prestação de Contas).

É imprescindível que os princípios do GDPR sejam plenamente conhecidos e aplicados, sem exceção, por desenvolvedores e projetistas de software em seus projetos, uma vez que a escassez dos mesmos em aplicações de software acarretam em violações de dados dos usuários [17]. Dessa forma, deve haver a esquematização das dificuldades relatadas pelos profissionais na tentativa de aplicar os princípios do Artigo 5, seja pela falta de familiaridade em relação a algum princípio específico do regulamento ou pela incompreensão acerca das técnicas de aplicação para se alcançar a implementação das diretivas.

Outrossim, a gestão das organizações responsáveis pelos profissionais impactam diretamente no artefato gerado, visto que problemas internos como a falta de recursos e guias específicos para a aplicação e priorização de requerimentos funcionais em detrimento da segurança/privacidade [17]. Destarte, as questões relatadas devem ser tratadas, a fim de realizar recomendações aos profissionais e organizações, além de fomentar discussões como a internacionalização da GDPR, a fim de que parâmetros de respeito a privacidade e proteção de dados pessoais sejam estabelecidos globalmente [17].

2.2.2 Lei Geral de Proteção de Dados Pessoais

A Lei Geral de Proteção de Dados Pessoais (LGPD) — Lei n° 13.709 —, ratificada em 14 de agosto de 2018 e já em vigor desde 14 de agosto de 2020 [14], obteve suas sanções administrativas em vigor em 1° de agosto de 2021 [47]. Embasada no regulamento europeu GDPR, a lei surgiu com o intuito de precaver que novas violações de dados ocorram, dado que as leis brasileiras anteriores direcionadas ao tratamento de dados não obtiveram sucesso na garantia total da proteção de dados pessoais, inclusive no quesito de desenvolvimento de software [48]. Assim, apresentado no Art. 1°, *caput* [14], a LGPD decreta que a mesma:

> "dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural."

No parâmetro de Engenharia de Software, tem-se que o ciclo de vida do tratamento de dados pessoais segue a sequência de etapas: coleta, retenção, processamento, compartilhamento e retenção, respectivamente [16]. A LGPD aborda o tratamento de dados pessoais e, no Art. 5°, inciso X, são definidas as operações amparadas juridicamente que estão inclusas no tratamento dos dados [14]. Assim, é possível estabelecer uma referência entre as cinco etapas do ciclo de vida do tratamento de dados pessoais e as respectivas operações da LGPD, como apontado pela Figura 2.3. Vale destacar que a operação de acesso está presente em todas as etapas do ciclo de vida, uma vez que é trivial para quaisquer operações. Ainda no Art. 5°, nos incisos I-III, a LGPD apresenta três conceitos referentes ao tipo de dado a ser tratado, que são eles [14]:

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

- 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.

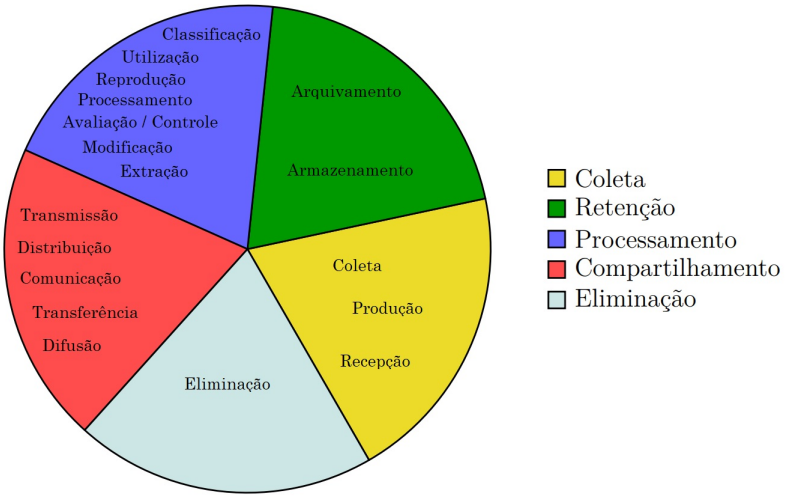

Figura 2.3: Relação entre fase do ciclo de vida do tratamento e operações da LGPD [14], [16].

Em complemento, entende-se que o dado pessoal sensível deve ser anonimizado para que seja desvinculado de uma pessoa natural, isto é, ela deixa de ser identificável a partir do dado e não é mais necessário ser amparada pela LGPD. A lei também conceitua, no inciso XI, o processo de anonimização, que se trata da utilização de técnicas que desvinculam a imagem associativa de um indivíduo ao dado exposto, utilizado em massa para assegurar a privacidade de dados digitais [49]. Acerca dos fundamentos propostos pela LGPD, a fim de assegurar a proteção de dados pessoais, evidencia-se no Art. 2° [14]:

1. o respeito à privacidade;
2. a autodeterminação informativa;
3. a liberdade de expressão, de informação, de comunicação e de opinião;
4. a inviolabilidade da intimidade, da honra e da imagem;
5. o desenvolvimento econômico e tecnológico e a inovação;
6. a livre iniciativa, a livre concorrência e a defesa do consumidor; e

7. os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Embora aplicadas em contextos diferentes, nota-se certa semelhança com as leis de proteção das últimas gerações propostas por Mayer-Schönberger [30] e, no parâmetro digital, os princípios do *Privacy by Design* [39]. A autodeterminação informativa, a título de exemplo, é reafirmada na LGPD, de modo a dedicar a um cidadão — também chamado de titular — o domínio sobre os seus dados.

Com relação aos responsáveis pelo tratamento dos dados pessoais, a LGPD sintetiza duas entidades: o controlador e o operador. O primeiro refere-se a pessoa física ou jurídica responsável por deliberar questões sobre o tratamento de dados e o último é o encarregado do controlador, que pode ser um desenvolvedor de software, de modo a efetivar o tratamento de dados. Ambas entidades são referenciadas como agentes de tratamento pela LGPD e estão passíveis à sanções administrativas em caso de violação das normas de tratamento de dados pessoais, que são aplicadas pela Autoridade Nacional de Proteção de Dados (ANPD), vide Capítulo IX da lei [14]. Assim, fica evidente o encargo da ANPD de fiscalizar o acatamento da LGPD.

Além dos fundamentos, no Art. 6° da LGPD são estabelecidos uma série de princípios — dez, em sua totalidade — que se refere à determinação do tratamento de dados adequado [14]. São eles, juntamente da respectiva descrição:

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.

Em relação à semelhança da robusta aplicação entre a LGPD e o GDPR têm-se, a titulo de exemplo, a aplicação da LGPD para quaisquer operações de tratamento que sejam realizadas em território nacional (vide Art. 3°) [14]. Assim como o GDPR [44], a LGPD se estende a empresas estrangeiras que se relacionam com o Brasil, ainda que o processamento de dados ocorra exteriormente, uma vez que basta que a coleta de dados tenha sido realizada no país [14]. Vale, então, a vasta aplicação da lei para países que se relacionam com o Brasil.

2.3 Trabalhos Correlatos

O estudo feito por Alhazmi et al. [17] identificou os principais pontos que impedem os desenvolvedores de software de colocarem em prática os princípios de preservação de privacidade presentes no GDPR em seus sistemas de software. Os principais pontos encontrados foram: falta de boas técnicas de implementação de privacidade, a falta de familiaridade com os princípios presentes no GDPR, a maior preocupação com a funcionalidade do que com a privacidade, falta de recursos e guias para implementação de privacidade e a falta de preocupação com privacidade por parte dos clientes.

Okano et. al [50] discutiram sobre as adaptações que as empresas e organizações tiveram de sofrer para se adequar a LGPD, assim como sobre possíveis *frameworks* para analisar se os procedimentos com dados pessoais também estão de acordo com a lei. A importância deste trabalho está relacionado com o fato de que modelos e *frameworks* podem facilitar o diagnóstico dos processos relacionados a LGPD.

Diante de um cenário de *Smart Cities* e no crescimento de dispositivos IOT (*Internet of Things*), Gheisari et al. [51] realizaram um estudo para propor um *framework* a fim de tentar resolver os problemas relacionados privacidade de dados gerados por dispositivos

IOT. Além de tratar da privacidade, o estudo também se relaciona com a heterogeneidade dos dados e o fornecimento de serviços de alto nível. A abordagem do *framework* proposto demonstrou-se eficaz no quesito de *Smart Cities*. Em contrapartida, não aborda os princípios específicos da GDPR.

Pensando não apenas em analisar a GDPR como uma lei que pune o uso incorreto de dados pessoais, Cormack et al. [52] realizaram uma análise sobre a GDPR como uma guia para o melhor desenvolvimento de softwares, visando processamento de dados. Analisando três contextos reais de processamento de dados, os autores demonstram como a GDPR pode ser vista como um rico material para embasar o design de sistemas de software de processamento de dados. Além de tornar o uso de dados pessoais mais seguros, também torna a produção desses sistemas de software mais eficaz e confiável.

Como resultado da criação da LGPD, Canedo et al. [12] propuseram um processo de implementação da LGPD utilizando o modelo BPMN (*Business Process Model and Notation*) para facilitar a implementação da LGPD pelas agências de administração do governo federal brasileiro. Além disso, o trabalho aborda maneiras de ensinar os trabalhadores dessas agências sobre as leis de proteção e regulamentação dos dados, entretanto, sem analisar os empecilhos que os atuais desenvolvedores possuem para tal implementação.

Ainda em um cenário de adaptação à LGPD por parte dos profissionais da área, Castro et al. [53] propõem um *framework*, embasado em uma metodologia que foi desenvolvida por profissionais brasileiros, denominada BEST (*Business Engaged Security Transformation*). O intuito é de parametrizar a adoção dos princípios da LGPD pelas organizações, a fim de que entrem em conformidade. Outrossim, o estudo apresenta um comparativo que estabelece a relação direta entre os princípios do *Privacy by Design* e os respectivos artigos da LGPD. Não obstante a implementação dos princípios da LGPD por parte das organizações, uma limitação do estudo foi a falta de treinamento dos empregados em relação à privacidade e proteção de dados.

Haja vista a implementação dos princípios da LGPD no setor público, especificamente, Canedo et al. [54] avaliam o cumprimento das diretrizes por parte de agências que compõem a Administração Pública Federal. Assim sendo, por meio da metodologia de pesquisa exploratória, na qual apenas funcionários do setor público foram avaliados, e da estratégia de triangulação dos dados coletados, foi possível relatar que os funcionários, majoritariamente, não dispunham das informações dos usuários livremente e deveriam apresentar conformidade com a lei.

Com o intuito de averiguar a interpretação, especialmente, de equipes de Desenvolvimento Ágil de Software, Canedo et al. [55] investigam a capacidade de aplicação dos profissionais — estes do setor público, do setor privado, envolvidos em projetos de pesquisa, etc. — dos princípios da LGPD na etapa de elicitação de requisitos de privacidade.

Um dos pontos mais relevantes retratados pela pesquisa foi a influência tanto de fatores internos, como a noção dos princípios mas sem a devida aplicação dos mesmos, e de fatores externos aos profissionais, como a dependência de especificações não otimizadas ou desatualizadas, propostas pelos *stakeholders*.

Canedo et al. [56] investigaram profissionais das áreas de Tecnologias da Informação e Comunicação (TIC) acerca da atuação e conformidade em relação aos princípios da LGPD por parte de suas respectivas organizações. A pesquisa revelou que há princípios que não são aplicados em sua completude, isto é, costumam ser negligenciados pelas organizações, de modo que uma parcela quase total já havia sofrido sanções administrativas por parte do órgão responsável, a Agência Nacional de Proteção de Dados (ANPD). Uma vez que não se tratava do escopo do projeto, houve a limitação a se entender o problema, e não sugerir possíveis implementações aos responsáveis pelas organizações.

A partir disso, o trabalho disposto busca identificar os principais pontos que carecem da atenção dos desenvolvedores de software — assim como o exposto por Alhazmi et. al [17] com foco na GDPR — para que suas aplicações estejam em concordância com os Artigos da LGPD, no quesito de privacidade de dados.

2.4 Síntese deste Capítulo

Este capítulo iniciou pela explicação de conceitos relacionados à privacidade e pela abordagem histórica de leis de privacidade de dados. Em seguida, apresentou os princípios e limites iniciais da privacidade através dos Princípios de Práticas de Informações Justas, e os requisitos de privacidade no desenvolvimento de software através do *Privacy by Design*. Por fim, apresentou as leis vigentes de proteção de dados pessoais europeia (GDPR) e brasileira (LGPD), bem como a diferença básica entre elas e como os desenvolvedores de software se relacionam com as mesmas.

Capítulo 3

Metodologia

Neste capítulo será apresentada a metodologia em amplo detalhamento, de modo que: a Seção 3.1 aborda a preparação experimental, isto é, a demarcação do escopo do estudo e como é realizado; a Seção 3.2 expõe o desenvolvimento de um cenário adequado e métodos adotados para verificar individualmente a aplicação dos princípios da Lei Geral de Proteção de Dados (LGPD) em um caso de uso — com o intuito de especificar um problema habitual — e a elaboração do *survey* para dado cenário; e a Seção 3.3 formaliza a análise a partir dos questionários realizados, pelo processo de teoria fundamentada [57]. Para a revisão de literatura e posterior discussão acerca do tema, foram-se utilizadas bibliotecas digitais, tais como *Google Scholar*, *Springer*, *DBLP*, *ArXiv*, *Taylor & Francis Online*, *IEEE Xplore*, entre outras.

O estudo visa identificar os desafios apresentados pelos desenvolvedores e projetistas de software durante a implementação dos princípios da LGPD em suas respectivas aplicações e, não obstante, propor um guia referencial posteriormente para auxiliar os profissionais diante os obstáculos.

3.1 Configuração Experimental do Estudo

Para participar da pesquisa foram convidados desenvolvedores de software com perfis variados, tanto em idade, quanto em experiência profissional. Uma vez que o problema de implementação de privacidade advém tanto por parte de desenvolvedores iniciantes quanto dos mais experientes — e até mesmo entre especialistas [58] —, faz-se necessário garantir que, independente do tempo de experiência, todo participante da pesquisa tenha sua resposta analisada. O único requisito necessário para participar da pesquisa é ser um desenvolvedor ou um projetista de software, de modo a correlacionar as práticas de design e arquiteturas de software aplicadas.

Acerca dos meios utilizados para divulgação da pesquisa, a principal plataforma utilizada foi a rede social LinkedIn, uma vez que possibilita o contato direcionado apenas aos profissionais da área. Ademais, para obter um maior alcance, o *survey* foi divulgado em outras plataformas, tais como grupos compostos por profissionais da área de computação dispostos no Facebook e no Microsoft Teams, inclusive naqueles focados especificamente em estudo da LGPD.

Para investigar tais dificuldades foram criados: um cenário de aplicação de software que propõe todos os princípios da LGPD; diagramas UML (*Unified Modeling Language*) desta mesma aplicação, com o intuito de refletir os princípios da LGPD; e um *survey* para obter as respostas dos participantes da pesquisa sobre como eles implementariam a aplicação proposta em cada quesito. Desse modo, após o consentimento dos participantes, houve a leitura e compreensão do cenário de aplicação de software descrito e dos diagramas UML. Por fim, os participantes responderam ao questionário proposto, de modo totalmente assíncrono, a fim de reduzir o tempo de espera entre a aplicação dos questionários e a análise dos resultados. O intuito da utilização dos *surveys* é avaliar se a possível implementação do software proposto está em conformidade com as práticas de boa-fé, e princípios de privacidade propostos pela LGPD [14].

3.2 Desenvolvimento do Cenário e Procedimentos

O cenário proposto para que os participantes discorram acerca dos princípios da LGPD é uma aplicação *online*, ou mais especificamente, uma aplicação *web*, que executa a função de um comércio eletrônico. Os requisitos funcionais da plataforma são básicos, como o registro de novos usuários e a venda/compra de produtos, sejam eles novos ou usados. Acerca das funções relacionadas ao processo de autenticação, a aplicação permite o registro e o *login* por parte dos usuários, sendo que esses se especificam em dois tipos: o cliente, que pode realizar depósito monetário para converter em dinheiro que pode ser utilizado na aplicação e pode consultar produtos disponíveis na plataforma; e o vendedor, que pode realizar o saque do dinheiro disponível na aplicação para sua conta bancária e pode cadastrar produtos na plataforma, além de alterar as informações dos mesmos já cadastrados por ele. Ademais, é essencial que um usuário possua cadastro na plataforma para conectar-se e alterar suas informações da conta. A Figura 3.1 apresenta os casos de uso dos usuários do sistema, que foram modelados em um diagrama de caso de uso UML.

Além das funcionalidades de autenticação e as previamente abordadas em uma circunstância anterior ao comércio propriamente dito, a relação entre usuários dentro da plataforma, isto é, cliente e vendedor, também deve ser elucidada. Um cliente, a título de exemplo, não deve possuir permissão para interagir em compras de outros clientes,

do mesmo modo que um vendedor não deve interferir em pedidos de outros vendedores. Dessa forma, sistematicamente, tem-se:

1. Cabe ao vendedor anunciar um ou mais produtos na plataforma, cada qual com sua respectiva descrição e preço;
2. Cabe ao cliente a escolha de um ou mais produtos anunciados e, posterior solicitação dos mesmos;
3. O vendedor, então, poderá checar os pedidos solicitados pelos clientes, enquanto que o cliente poderá verificar as informações da compra a ser realizada, que serão enviadas pelo vendedor;
4. Uma vez que ambos expressam concordância: o cliente poderá prosseguir para a confirmação da compra e posterior realização do pagamento; e o vendedor receberá o pagamento.

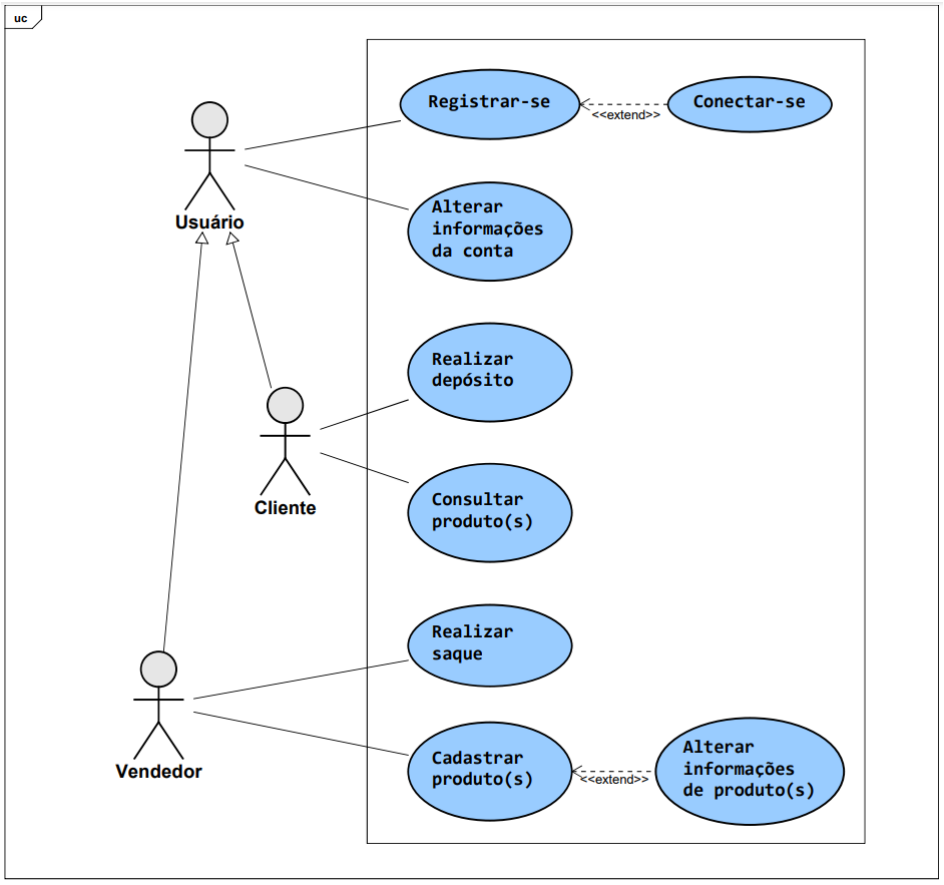

Figura 3.1: Casos de uso dos usuários do sistema.

A integração das funcionalidades do sistema de compras é regida por múltiplos requisitos funcionais, de modo que os requisitos de privacidade devam ser considerados (sem

exclusão dos requisitos de segurança, com aplicação de diretivas criptográficas). Assim, os requisitos são igualmente modelados em um diagrama de caso de uso UML, conforme apresentado na Figura 3.2.

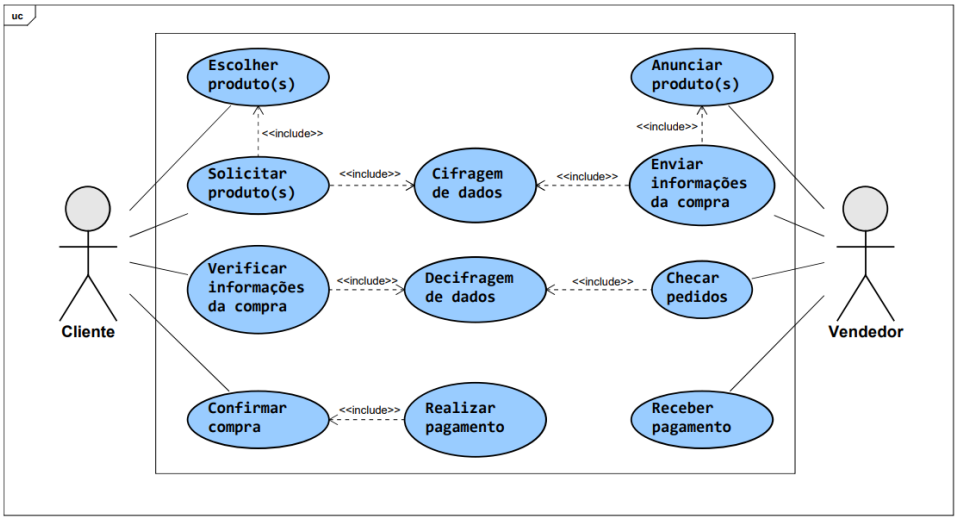

Figura 3.2: Casos de uso de compras *online* no sistema.

Uma vez estabelecido o respectivo cenário e seus procedimentos, foi destacada a relação entre cada princípio da LGPD e o ambiente a ser desenvolvido, a fim de que questionamentos pontuais pudessem ser realizados para cada participante do *survey*. O intuito é que, para todo princípio incluso no Art. 6 ° [14], ocorra a exclusividade da verificação da conformidade dos participantes em relação a cada um dos incisos, mas também a aspectos inter-relacionados na lei. Para cada princípio da LGPD, é abordado os pontos de questionamento relativos ao cenário criado, que devem ser elucidados por todos os participantes, e são eles:

1. Finalidade: é solicitado aos participantes que expliquem como será garantido que os dados do sistema de compras e vendas *online* sejam tratados de maneira legítima, de modo que os usuários saibam a finalidade do tratamento de suas informações. Além disso, por se tratar de aplicações legítimas, é requisitado aos participantes que discorram sobre técnicas para garantir a impossibilidade do tratamento dos dados para fins não especificados, isto é, fins que não sejam compatíveis com os legitimados previamente no sistema. É almejado que os participantes estejam em conformidade com as hipóteses correspondentes à coleta dos dados, vide Artigos 7° e 11°, além da previsão legal e finalidade, como consta no Artigo 23°, inciso I [14];

2. Adequação: é solicitado aos participantes que descrevam quais métodos/técnicas serão utilizados para a implementação da limitação contextual dos dados, isto é, a

compatibilidade do tratamento no escopo especificado pela finalidade e o armazenamento dos dados pessoais no sistema somente enquanto necessário. Espera-se que os meios de implementação apresentados sejam compatíveis e tão somente com as finalidades explicitadas;

3. Necessidade: é solicitado aos participantes que abordem quais dados deverão ser coletados em cada caso de uso do sistema, de modo que não extrapole o mínimo necessário em relação às finalidades. Ademais, é requerido que os participantes explicitem possíveis técnicas para essa limitação do tratamento dos dados, a fim de que estejam relacionados apenas dados pertinentes, proporcionais e não excessivos às finalidades, isto é, dados condizentes com os fins explicitados;

4. Livre acesso: é solicitado aos participantes que expliquem como será garantido que os usuários do sistema possam consultar quaisquer etapas de tratamento dos seus dados, bem como o modo em que são utilizados e a duração do tratamento. Além disso, é almejado que os participantes explicitem as técnicas a serem empregadas para a disponibilização de informações aos usuários, que deve ser gratuita e de fácil acesso, tal qual acerca da integralidade dos dados pessoais;

5. Qualidade dos dados: é solicitado aos participantes que expliquem como serão garantidas a integralidade, a clareza e a indispensabilidade dos dados e suas atualizações no sistema. É almejado que os participantes apresentem técnicas que inviabilizem acessos ilegítimos aos dados dos usuários, sejam por outros usuários ou por agentes externos, a fim de garantir a exatidão dos dados apresentados;

6. Transparência: é solicitado aos participantes que expliquem como todo usuário do sistema, tanto o cliente quanto o vendedor, poderão se informar integralmente acerca da realização do tratamento de seus dados, bem como os agentes de tratamento envolvidos — o controlador e o operador, vide Art. 5°, inciso IX — e as operações por eles realizadas, como consta no Art. 37° [14]. É almejado que os participantes exponham técnicas que garantam a integralidade, a transparência e a usabilidade das informações a serem apresentadas aos usuários;

7. Segurança: é solicitado aos participantes que expliquem como irão salvaguardar os dados pessoais de acessos não autorizados, tanto no processo de autenticação no sistema, quanto no processo de compras *online*. Além disso, é pedido aos participantes que elucidem técnicas protetivas que garantam a integridade — a fim de evitar eliminação e perda dos dados — e a confidencialidade — a fim de evitar o processamento e compartilhamento de informações — dos dados pessoais no sistema apresentado, mesmo que ocorram situações acidentais. Espera-se que os participan-

tes apontem técnicas que impeçam o acesso não autenticado em cada caso de uso, como a utilização de métodos criptográficos específicos;

8. Prevenção: é solicitado aos participantes que apontem as medidas a serem implementadas que, durante o tratamento dos dados pessoais, impeçam a ocorrência de danos, nos casos de uso dos usuários do sistema e nos casos de uso de compras *online*. Espera-se que os participantes ressaltem técnicas preventivas de proteção, e não reativas.

9. Não discriminação: é solicitado aos participantes que expliquem como impossibilitarão o tratamento discriminatório ilícito ou abusivo no processo de autenticação dos usuários e no processo de compra *online*. Ademais, é pedido que informem como permitirão que os usuários possam realizar requisições em caso de discordância do tratamento adotado, inclusive em meios de tratamento automatizados, como consta no Art. 20°, parágrafo 2° [14]. É almejado que os participantes utilizem medidas especiais para dados pessoais sensíveis, como a pseudonimização.

10. Responsabilização e prestação de contas: é solicitado aos participantes que expliquem como será garantida a conformidade do sistema com as diretrizes da LGPD em relação à proteção dos dados pessoais de cada um dos usuários. É almejado que os participantes ressaltem medidas efetivas de comprovação do comprometimento dos agentes de tratamento, da rastreabilidade e ainda, em caso de danos, de reparação dos mesmos, como consta no Art. 42°, *caput* [14].

3.2.1 Elaboração do *Survey*

O desenvolvimento do questionário com base no cenário especificado pode ser dividido em duas finalidades:

- As perguntas Q01 a Q06, vide Tabela 3.1, são relativas a compreensão do perfil do participante, as quais vão desde de informações para a associação de um indivíduo até a área de atuação e experiência profissional;
- As perguntas Q07 a Q40, vide Tabelas 3.2, 3.3, 3.4 e 3.5, são relativas a averiguação da conformidade do participante com cada princípio da LGPD, dado o cenário proposto.

Tabela 3.1: Perguntas direcionadas ao perfil do participante.

ID	Pergunta	Escala de resposta
Q01	Qual é o seu nome?	Em aberto.
Q02	Qual é a sua idade?	Menos de 21 anos; entre 21 a 25 anos; entre 26 a 30 anos; entre 31 a 35 anos; entre 36 a 40 anos; entre 41 a 45 anos; entre 46 a 50 anos; entre 51 a 55 anos; entre 56 a 60 anos; mais de 60 anos.
Q03	Qual é o seu nível de escolaridade?	Graduando; graduado; especialização; mestrado; doutorado.
Q04	Em qual etapa de desenvolvimento de software você trabalha profissionalmente?	Elicitação de requisitos; análise de dados; modelagem de sistemas; desenvolvimento/programação; testes; manutenção e evolução de software; outro.
Q05	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.
Q06	Acerca da questão de privacidade de dados, você se considera familiar em relação à Lei Geral de Proteção de Dados.	Resposta em escala de *Likert*: concordo plenamente; concordo parcialmente; não concordo, nem discordo; discordo parcialmente; discordo plenamente.

Tabela 3.2: Perguntas direcionadas a conformidade do participante com a LGPD parte 1.

ID	Pergunta	Escala de resposta	Princípio
Q07	No cenário do comércio eletrônico, você sabe como faria para que os clientes e os vendedores saibam o motivo da coleta de seus dados? Seria utilizada alguma técnica específica?	Em aberto.	Finalidade.
Q08	Você sabe como faria para garantir que os dados coletados não sejam tratados de maneira alheia ao motivo especificado para os usuários? Se sim, poderia descrever?	Em aberto.	Finalidade.
Q09	Você já implementou essa funcionalidade, em alguma aplicação, de se limitar apenas à finalidade declarada aos usuários? Se sim, quais foram as dificuldades encontradas? Se não, poderia dizer o motivo pelo qual não implementou?	Em aberto.	Finalidade.
Q10	No cenário do comércio eletrônico, você conhece técnicas para assegurar que o tratamento dos dados dos usuários seja consistente com o objetivo no processo de autenticação? E no processo de compra?	Em aberto.	Adequação.
Q11	Você já implementou, em alguma outra aplicação, a funcionalidade de assegurar que o tratamento dos dados seja consistente com o objetivo no processo de autenticação anteriormente? Se sim, quais foram as dificuldades encontradas? Se não, poderia dizer o motivo pelo qual não implementou?	Em aberto.	Adequação.
Q12	Você removeria os dados de usuários que estão armazenados no sistema e não são mais estritamente necessários?	Resposta em escala de *Likert*.	Necessidade.
Q13	Você conhece alguma técnica para remover os dados de usuários que estão armazenados no sistema e não são mais estritamente necessários? Se sim, poderia descrevê-la?	Em aberto.	Necessidade.
Q14	No cenário do comércio eletrônico, quais dados seriam coletados dos clientes e dos vendedores em um processo de autenticação? E em um processo de compra?	Em aberto.	Necessidade.
Q15	Você considera que todos os dados a serem coletados anteriormente são estritamente necessários para o funcionamento do sistema?	Resposta em escala de *Likert*.	Necessidade.
Q16	Você conhece técnica(s) para limitar a coleta de dados apenas ao estritamente necessário? Se sim, poderia descrevê-la(s)?	Em aberto.	Necessidade.
Q17	Você acha que haveria alguma dificuldade em definir quais seriam os dados estritamente necessários?	Resposta em escala de *Likert*.	Necessidade.
Q18	No cenário do comércio eletrônico, você conhece alguma técnica que poderia ser utilizada para assegurar que os clientes e os vendedores possam consultar como seus dados estão sendo utilizados? Se sim, poderia descrevê-la?	Em aberto.	Livre acesso.

Tabela 3.3: Perguntas direcionadas a conformidade do participante com a LGPD parte 2.

ID	Pergunta	Escala de resposta	Princípio
Q19	Você já implementou a funcionalidade explicitada anteriormente, que assegura que os clientes e vendedores possam consultar como seus dados estão sendo utilizados? Se sim, quais foram as dificuldades encontradas? Se não, poderia dizer o motivo pelo qual não implementou?	Em aberto.	Livre acesso.
Q20	No cenário do comércio eletrônico, você conhece alguma técnica que poderia ser utilizada para garantir que os dados presentes no sistema representam com exatidão, isto é, estão corretos e atualizados, os dados dos usuários? Se sim, poderia descrevê-la?	Em aberto.	Qualidade dos dados.
Q21	Você conhece técnica(s) de implementação para impedir que pessoas não autorizadas possam visualizar ou interagir com dados de quaisquer usuários? Se sim, poderia descrevê-la(s)?	Em aberto.	Qualidade dos dados.
Q22	Você já implementou a funcionalidade, explicitada anteriormente, que impede que pessoas não autorizadas possam visualizar ou interagir com dados de quaisquer usuários? Se sim, quais foram as dificuldades encontradas? Se não, poderia dizer o motivo pelo qual não implementou?	Em aberto.	Qualidade dos dados.
Q23	No cenário do comércio eletrônico, você conhece alguma técnica que poderia ser utilizada para notificar clientes e vendedores sobre todas as etapas de tratamento dos seus dados? Se sim, poderia descrevê-la?	Em aberto.	Transparência.
Q24	Você considera importante o registro no sistema de cada operação realizada pelos agentes de tratamento?	Resposta em escala de *Likert*.	Transparência.
Q25	Você já implementou, em alguma aplicação, uma funcionalidade que registra cada operação realizada no tratamento de dados dos usuários, inclusive os responsáveis pela operação? Se sim, quais foram as dificuldades encontradas? Se não, poderia dizer o motivo pelo qual não implementou?	Em aberto.	Transparência.
Q26	No cenário do comércio eletrônico, você conhece métodos a serem utilizados no processo de autenticação de um usuário para garantir a segurança? E no processo de compra *online*? Se sim, poderia descrevê-los?	Em aberto.	Segurança.
Q27	Você conhece técnicas que poderiam impedir o vazamento de informações de clientes e vendedores? E uma possível alteração não autorizada desses dados? Se sim, poderia descrevê-las?	Em aberto.	Segurança.
Q28	Suponha que ocorra um vazamento de dados. Você conhece alguma técnica para garantir que as informações vazadas não comprometam a privacidade dos usuários? Se sim, poderia descrevê-la?	Em aberto.	Segurança.

Tabela 3.4: Perguntas direcionadas a conformidade do participante com a LGPD parte 3.

ID	Pergunta	Escala de resposta	Princípio
Q29	Você já implementou técnicas de segurança anteriormente? Se sim, quais foram as dificuldades encontradas? Se não, poderia dizer o motivo pelo qual isso ocorreu e se houve algum problema posteriormente?	Em aberto.	Segurança.
Q30	No cenário do comércio eletrônico, você conhece medidas para garantir que, nos processos de autenticação e de compra *online*, não venham a ocorrer danificação na integridade dos dados?	Em aberto.	Prevenção.
Q31	Você implementaria essa garantia da integridade dos dados de modo preventivo ou reativo aos danos?	Preventivo; Reativo.	Prevenção.
Q32	Você já implementou uma funcionalidade, em alguma outra aplicação, que evita que os dados sejam danificados durante alguma operação? Se sim quais foram as dificuldades encontradas? Se não, poderia dizer o motivo pelo qual não foi necessário implementar?	Em aberto.	Prevenção.
Q33	No cenário do comércio eletrônico, você conhece alguma técnica que poderia ser utilizada para impedir o tratamento enviesado, isto é, o tratamento discriminatório dos dados de clientes e vendedores?	Em aberto.	Não discriminação.
Q34	Com relação ao tratamento de dados pessoais sensíveis, você conhece algum método para impedir um possível tratamento discriminatório? Se sim, poderia descrevê-lo?	Em aberto.	Não discriminação.
Q35	Em caso de discordância, por parte de algum usuário, da licitude do tratamento adotado, você conhece algum método para permitir que os mesmos façam requisições aos responsáveis? Se sim, poderia descrevê-lo?	Em aberto.	Não discriminação.
Q36	Você já implementou, em alguma aplicação, a funcionalidade que permite a realização de requisições aos responsáveis, por parte dos usuários, em caso de discordância do tratamento adotado? Se sim, quais foram as dificuldades encontradas? Se não, poderia dizer o motivo pelo qual isso ocorreu?	Em aberto.	Não discriminação.
Q37	No cenário do comércio eletrônico, você conhece medidas que adotaria para garantir a rastreabilidade dos responsáveis pelo tratamento de dados dos usuários em relação ao cumprimento das normas? Se sim, poderia dizer como isso seria feito?	Em aberto.	Responsabilização e prestação de contas.

Tabela 3.5: Perguntas direcionadas a conformidade do participante com a LGPD parte 4.

ID	Pergunta	Escala de resposta	Princípio
Q38	Você conhece medidas para mensurar a eficácia do tratamento adotado por parte dos responsáveis? Se sim, poderia citá-las?	Em aberto.	Responsabilização e prestação de contas.
Q39	Você considera importante manter a rastreabilidade enquanto durar o processo do tratamento dos dados?	Resposta em escala de *Likert*.	Responsabilização e prestação de contas.
Q40	Você já implementou, em alguma outra aplicação, a funcionalidade de rastreabilidade dos responsáveis, enquanto durar o processo de tratamento dos dados? Se sim, quais foram as dificuldades encontradas? Se não, poderia dizer o motivo pelo qual não foi necessário?	Em aberto.	Responsabilização e prestação de contas.

3.3 Análise dos Dados

Para uma análise compreensiva dos dados a partir dos questionários, foi utilizada a prática de teoria fundamentada, focalizada na área de Engenharia de Software [59]. Por meio dessa técnica aplicada em questões de resposta livre, foi possível parametrizar a conformidade dos participantes acerca de cada princípio da LGPD, de modo que houve uma divisão das etapas de análise. A Figura 3.3 ilustra os passos que foram adotados, desde a coleta dos dados pelo *survey*, até a elaboração do guia referencial.

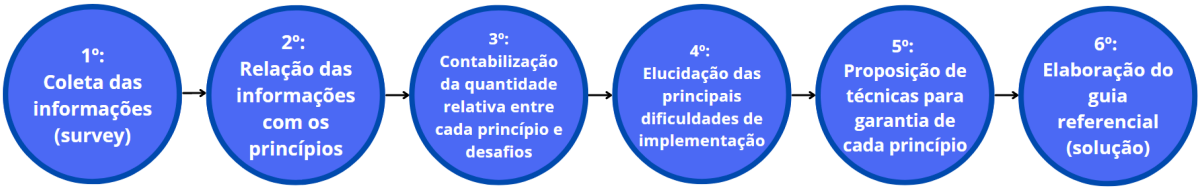

Figura 3.3: Etapas de análise dos dados pela utilização da teoria fundamentada.

Dessa forma, através do percurso adotado, na 1ª etapa há ocorrência somente da coleta das respostas do questionário, em que a maioria é referente às questões de resposta livre. A 2ª etapa é considerada a mais importante pela técnica utilizada, uma vez que permite identificar padrões ainda que em um nível de análise complexo, isto é, em respostas que não possuem escala definida.

Em seguida, na 3ª etapa, é possível quantificar e ordenar os princípios em escala de dificuldade, a fim de mensurar quais foram considerados de difícil implementação pelos participantes. A 4ª etapa possibilita uma especificação da etapa anterior, isto é, realizar um tabelamento das dificuldades respectivas a cada princípio.

Já na elaboração de uma solução, a 5ª etapa trata da proposição de técnicas funcionais, a fim de que sejam utilizadas em prática, e a 6ª etapa focaliza na criação de um guia que relaciona as técnicas com possíveis implementações, respectivamente.

3.4 Síntese deste Capítulo

Este capítulo iniciou pela explicação da configuração experimental do estudo, isto é, o desígnio que o atual trabalho propõe estudar, como participantes envolvidos, ferramentas utilizadas e metodologia a ser seguida. Em seguida, apresentou o cenário elaborado para a pesquisa e como cada princípio da LGPD há de ser averiguado, bem como o desenvolvimento de um questionário para posterior análise qualitativa. Por fim, apresentou como os dados foram analisados, isto é, desde a coleta até a elaboração do guia referencial, proposto no capítulo seguinte.

Capítulo 4

Resultados

Neste capítulo serão apresentados o desenvolvimento da pesquisa e as respectivas discussões, de modo que: a Seção 4.1 elucida uma análise dos resultados, isto é, uma comparação dos resultados obtidos no questionário com os explicitados na literatura; a Seção 4.2 expõe as limitações da pesquisa, que são os escopos de estudo relacionados ao projeto, mas que não foram abordados na pesquisa, além de abordar as ameaças para a validação do estudo e as respectivas técnicas utilizadas para mitigá-las; e a Seção 4.3 apresenta a proposição do guia referencial prático, para contribuição da conformidade dos profissionais de software em relação aos princípios da Lei Geral de Proteção de Dados (LGPD).

4.1 Análise do *Survey*

O *survey* continha 40 perguntas, Q01 a Q40, conforme apresentado na Tabela 3.5. O *survey* ficou disponível *online* por 4 semanas, de modo que foram obtidas 45 respostas e o tempo médio de resposta foi de 40 minutos. No momento da aplicação, os participantes puderam expor suas dúvidas e sugestões — inclusive foram motivados a isso — nas plataformas em que os questionários foram divulgados, a fim de que as questões pudessem ser aprimoradas com novas alternativas ou exemplificações. Acerca da análise das respostas, ambos os autores participaram, de modo que foi realizada a esquematização em uma planilha virtual para que fosse possível contabilizar com eficácia as respostas de cada questão.

No que se refere ao perfil demográfico dos respondentes, isto é, as questões Q02 e Q03, tem-se: a relação de idade, que é apresentada na Tabela 4.1 (note que não houve nenhum participante com margem de idade superior a 45 anos); e a relação do nível de escolaridade dos participantes, igualmente mostrado na Tabela 4.1, em que a grande maioria (aproximadamente 88,9%) não possui pós-graduação.

Tabela 4.1: Perfil dos participantes.

Idade (anos)		**Escolaridade**		**Estágio de desenvolvimento**	
Intervalo	%	**Nível**	%	**Etapa**	%
< 21	4,4	**Graduando**	53,3	**Desenvolvimento/Programação**	64,4
entre 21 e 25	62,2	**Graduado**	35,6	**Análise de Dados**	6,7
entre 26 e 30	24,4	**Especialização**	6,7	**Teste**	6,7
entre 31 e 35	2,2	**Mestrado**	4,4	**Elicitação de Requisitos**	4,4
entre 36 e 40	4,4			**Manutenção e Evolução de software**	2,2
entre 41 e 45	2,2			**Outro**	15,6

Haja vista a atuação profissional dos participantes, referente à questão Q04, mais da metade pertence às etapas de desenvolvimento e programação de software, vide Tabela 4.1. Vale lembrar que todos os respondentes possuem conhecimento em desenvolvimento/programação *web*. Todavia, a experiência pode influenciar em suas respostas focadas em conhecimento sobre LGPD. Assim, ao se questionar os participantes que responderam a última opção (Outro), foi informado que há contribuição profissional em mais de uma das etapas supracitadas, como seguem as transcrições abaixo:

> *"Ao invés de ser somente uma escolha, às vezes poderia ter sido um campo de múltipla escolha ou um campo de todas as opções, o que seria o meu caso."*

> *"[...] é mais de um dentre as opções que disponibilizaram, aí tive que escolher: Outro."*

Ainda no escopo profissional, a questão Q05 relata o tempo de experiência dos participantes, isto é, o tempo que ocupam cargos em organizações relacionados ao desenvolvimento de software, e segue de acordo com a Tabela 4.2. É possível observar que apenas 45% dos participantes, aproximadamente, trabalham há mais de 3 anos em seus cargos.

Tabela 4.2: Experiência profissional dos participantes.

Experiência (anos)	%
< 1	13,3
entre 1 e 3	42,2
entre 4 e 6	35,6
entre 7 e 9	6,7
> 9	2,2

Em relação à prévia do *survey*, os participantes foram questionados acerca da familiaridade com a LGPD, isto é, se estão a par das diretrizes da lei, vide questão Q06. Uma maioria de 73% dos participantes concordam ou concordam totalmente que estão a par da LGPD, 11% nem concordam ou discordam, e apenas 16% discordam ou discordam totalmente, a relação pode ser observada na Figura 4.1.

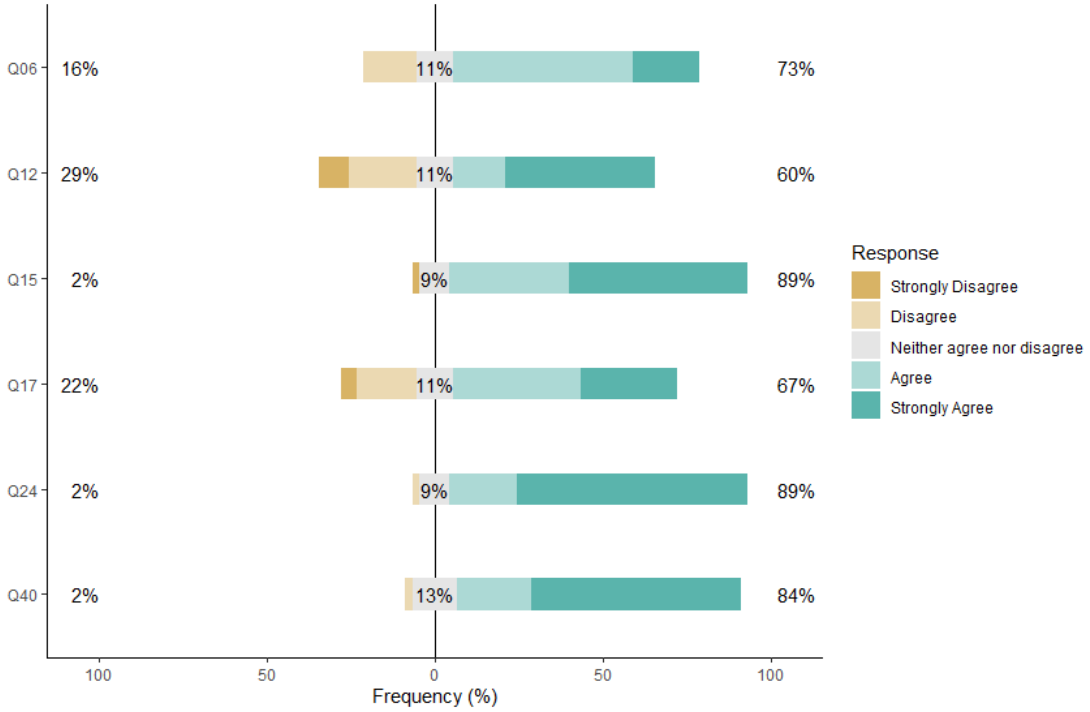

Figura 4.1: Escala *Likert* de concordância das questões do *survey*.

Isso significa que quase três-quartos dos respondentes afirmaram que se consideram familiarizados em relação à LGPD, sendo que nenhum dos participantes informou desconhecer totalmente a lei. Essa relação será averiguada ao final da subseção, além da comparação entre os princípios que os participantes apresentaram maior dificuldade em compreender ou implementar.

As respostas referentes às perguntas Q07, Q08 e Q09, que são respectivas à implementação do princípio da finalidade, são apresentadas na Figura 4.2. Assim, 55,6% (25/45) dos participantes demonstraram que estão em total conformidade com o princípio, isto é, conhecem técnicas para que os usuários da nossa aplicação *web* saibam o motivo da coleta de seus dados e, além disso, sabem como garantir que os dados não sejam tratados de maneira alheia ao especificado. Em contrapartida, 28,9% (13/45) dos respondentes ou não conhecem algum método, ou não sabem como garantir a efetividade do respectivo método, e 15,6% (7/45) não apresentaram uma solução válida. Acerca das técnicas de implementação informadas, a mais citada foi a utilização de Termo de Uso, seguida de Política de Privacidade e de Cookies.

Ao serem questionados sobre a prévia implementação da funcionalidade que garante que o princípio da finalidade seja respeitado, apenas 35,6% (16/45) dos participantes já haviam praticado, de modo que a maior dificuldade, mostrada na Tabela 4.3, foi a relação de estabelecer confiança com o usuário (e em deixar claro os motivos da coleta para o usuário).

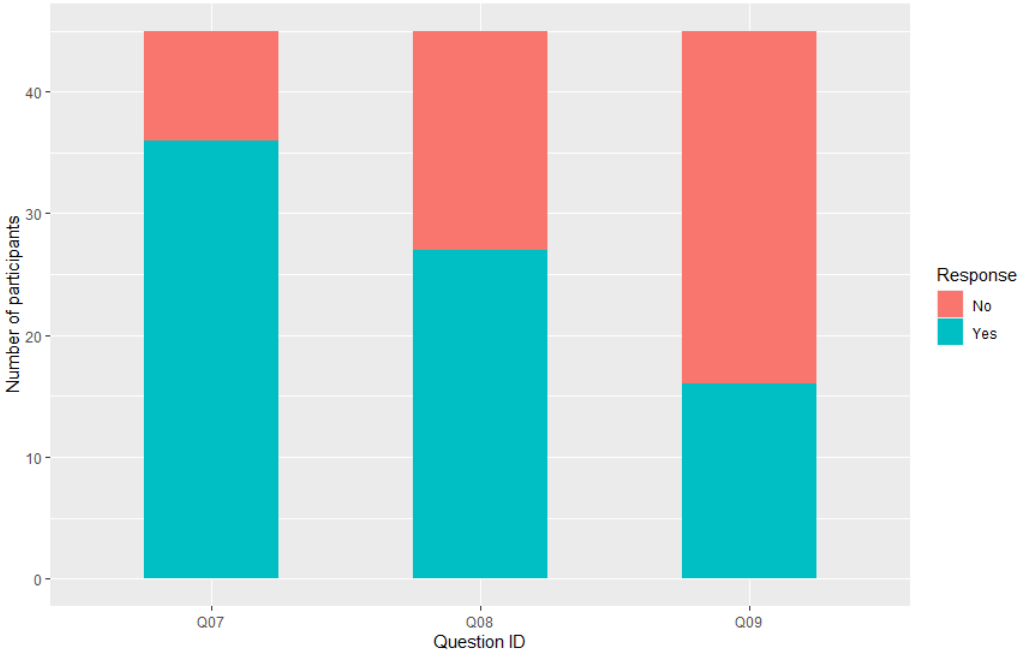

Figura 4.2: Conformidade dos participantes com o princípio de finalidade.

Tabela 4.3: Dificuldades de implementação do princípio de finalidade.

Dificuldade encontrada	#	%
Relacionamento com o usuário	4	25
Ferramenta utilizada	2	12,5
Limitação pela organização	2	12,5
Sem dificuldades	8	50

Por outro lado, 64,4% (29/45) nunca implementou, sendo que o motivo principal apontado pelos participantes, dispostos na Tabela 4.4, foram os de que ainda não têm conhecimento/experiência. É importante elucidar que essa também foi a maior adversidade encontrada pelos desenvolvedores na implementação de princípios da GDPR [17]). Além disso, quase um terço alegou que não era responsável por essa área de atuação. Ainda em menor quantidade, poucos desenvolvedores afirmaram que não implementaram pois não era necessário para a aplicação e um único profissional declarou que não constava nas normas gerais da empresa.

Tabela 4.4: Motivos da falta de implementação do princípio de finalidade.

Motivo apontado	#	%
Não tenho domínio	15	51,7
Não era minha responsabilidade	9	31
Não era um requisito funcional	4	13,8
Não foi permitido pela organização	1	3,4

Em relação ao princípio da adequação, referente às questões Q10 e Q11, esperava-se um cenário em que a maioria dos desenvolvedores não possuía conhecimento do princípio, haja vista o trabalho realizado por Canedo et al. [55], que explora a experiência de equipes ágeis em relação a LGPD. De fato, o atual estudo corrobora com essa ideia, uma vez que 64,4% (29/45) dos respondentes não conhecem técnicas que garantam que o tratamento dos dados seja adequado com as finalidades propostas, vide Figura 4.3.

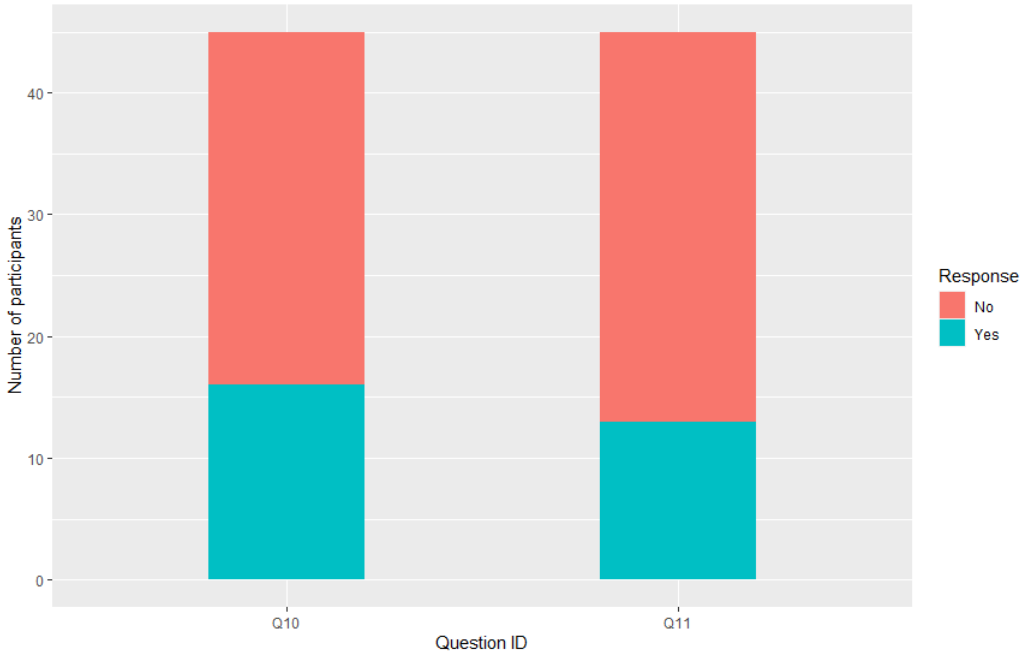

Figura 4.3: Conformidade dos participantes com o princípio de adequação.

A parcela dos participantes que conhecem técnicas que garantam o princípio da adequação — 35,6% (16/45) — informou métodos que variam desde a revisão das bases legais em cada um dos processo até o estabelecimento de políticas de segurança, no intuito de inviabilizar um tratamento incompatível com as finalidades.

No quesito de uma prévia implementação em outras aplicações, apenas 28,9% (13/45) dos respondentes já haviam realizado, de modo que mais da metade não encontrou dificuldade alguma, como mostrado na Tabela 4.5. Entretanto, o problema mais citado foi o de limitação pela organização, isto é, algum entrave proposto pela organização que dificulta a aplicação do princípio, tal como a maneira em que os dados estão estruturados e são armazenados.

Tabela 4.5: Dificuldades de implementação do princípio de adequação.

Dificuldade encontrada	#	%
Limitação pela organização	3	23
Ferramenta utilizada	2	15,4
Compreensão da funcionalidade	1	7,7
Sem dificuldades	7	53,8

Em contrapartida, uma maioria de 71,1% (32/45) nunca implementou uma funcionalidade que garanta o princípio da adequação, sendo que o principal motivo apontado foi a falta de compreensão do princípio (não houve familiaridade), como consta na Tabela 4.6. Em seguida, por não se tratar de um requisito funcional, houve participantes que optaram por não utilizar a funcionalidade, visto que poderia reduzir o desempenho da plataforma.

Tabela 4.6: Motivos da falta de implementação do princípio de adequação.

Motivo apontado	#	%
Não tenho domínio	23	71,9
Não era um requisito funcional	5	15,6
Não era minha responsabilidade	4	12,5

Acerca das questões Q13 e Q16 (mostradas na Figura 4.4), que abordam a conformidade dos respondentes com técnicas de implementação do princípio da necessidade, 26,7% (12/45) dos participantes demonstraram conhecer métodos que garantam por completo o princípio (para coleta de dados que sejam apenas estritamente necessários e para remoção dos que não sejam). Além disso, 28,9% (13/45) afirmaram não conhecer uma das duas técnicas, de modo que a maior dificuldade foi a descrição de um procedimento que cumpra a funcionalidade de remover dados que não são estritamente necessários.

Em controvérsia, 44,4% (20/45) relataram não saber ou não concordar com o princípio (motivados ou não por suas respectivas organizações). No geral, a discordância em remover dados que não são mais necessários é devido à dificuldade de se definir quais informações são relevantes e quais devem ser mantidas em cada contexto, como expresso nas transcrições de participantes a seguir:

> *"A necessidade de algo é imprevisível, só porque você não precisa de algo em um determinado momento não quer dizer que não vai precisar no futuro. Pode ser que seja necessário realizar uma auditoria no sistema, rever alguma transação ou investigar algum usuário."*

> *"Não conheço. Essa prática não é recomendada. Todos os dados são importantes, mesmo aqueles que possam não parecerem serem necessários. A equipe que roda script em produção é praticamente proibida de rodar "delete" no banco de dados."*

> *"Não concordo em remover os dados do banco de dados, isso causa inconsistência no banco. É melhor deixar eles inativos através de um booleano."*

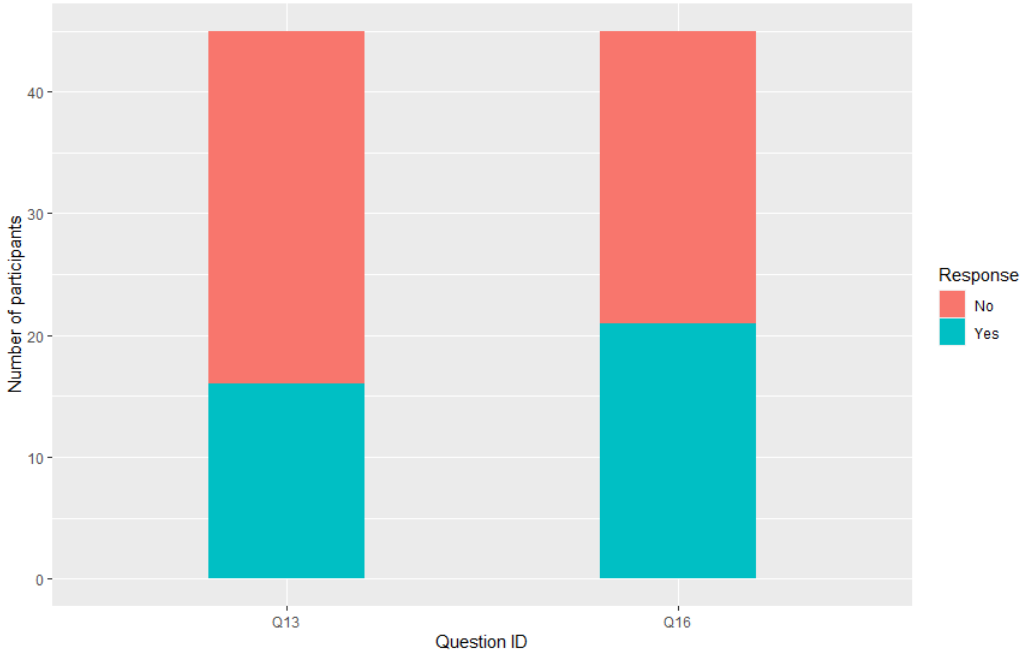

Figura 4.4: Conformidade dos participantes com o princípio de necessidade.

Em relação à questão Q14, que trata de quais dados deveriam ser coletados em um cenário de autenticação, a maior parte dos respondentes citou *e-mail* e senha. Além disso, outros poucos apresentaram interesse na coleta do nome e do CPF do usuário, o que poderia ser uma alternativa válida para o *e-mail*. No processo de compra, houve uma contraposição por parte dos respondentes. Uma parcela declarou a necessidade da coleta e armazenamento dos dados bancários de cada usuário, enquanto outros informaram que não se deve armazenar tais dados ou sequer são necessários para uso posterior (a consulta das informações do pagamento poderia ser realizada pelo endereço ou dado pessoal semelhante, que retorna um identificador para consulta do *status* do pagamento).

Em um quesito mais técnico, os respondentes ainda informaram a necessidade da coleta de *cookies* de autenticação, localização, endereço IP da rede e dados de *analytics*, tais como tempo de tela, fluxo de uso, etc. Além disso, um participante declarou que apesar de quaisquer dados que serão coletados, o usuário comumente tende a não se importar, como na transcrição abaixo:

> *"Ao final do dia somos é reféns dos sites/aplicativos que usamos, queremos usá-los mais do que nossa privacidade."*

Para as questões Q12, Q15 e Q17, que são perguntas relativas ao princípio da necessidade e que exigem respostas em escala *Likert*, a relação exibida se encontra igualmente exposta na Figura 4.1. As questões Q24 e Q40 são referentes aos princípios da transparência e da responsabilização e prestação de contas, e serão discutidas posteriormente.

É possível observar que 40% dos respondentes afirmam não concordar com a remoção de dados que não sejam estritamente necessários no sistema (e o respectivo impacto sobre a relação de conformidade com o princípio). Quase 90% concorda ou concorda totalmente que os dados escolhidos na questão Q14 são estritamente necessários para o funcionamento do sistema e ainda a maior parte (67%) concorda ou concorda totalmente que haveria dificuldades em definir todos os dados indispensáveis.

Adiante, para as questões Q18 e Q19 — que são respectivas ao princípio de livre acesso —, uma minoria de 40% (18/45) dos respondentes obtiveram êxito em responder adequadamente técnicas de consulta sobre os dados dos usuários, como disposto na Figura 4.5. Dentre os métodos mais citados, estão a política de privacidade e um registro das informações integrado ao perfil de cada usuário.

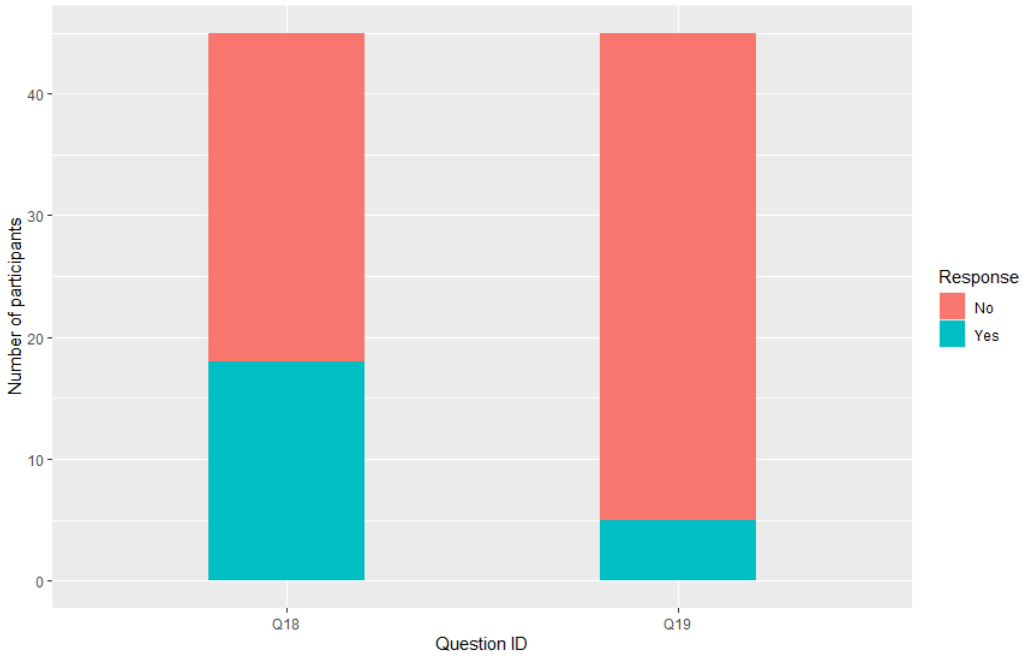

Figura 4.5: Conformidade dos participantes com o princípio de livre acesso.

Em relação à prévia implementação dessa funcionalidade em outras aplicações, foi o princípio que obteve a menor quantidade de participantes que já havia realizado, igualmente ao trabalho proposto por Canedo et al. [55]. Apenas 11,1% (5/45) dos participantes já implementaram, sendo que três afirmaram não tiveram dificuldades e dois expuseram problemas em relacionamento com o usuário. A porção de respondentes que não implementou — 88,9% (40/45) — informou que o motivo principal é que ainda não possuem prática ou completo entendimento do princípio, seguido de que não era um requisito funcional para a aplicação ou não era responsável pela funcionalidade (vide Tabela 4.7).

Tabela 4.7: Motivos da falta de implementação do princípio de livre acesso.

Motivo apontado	#	%
Não tenho domínio	29	72,5
Não era um requisito funcional	6	15
Não era minha responsabilidade	5	12,5

Em seguida, as perguntas Q20, Q21 e Q22 são respectivas ao princípio de qualidade dos dados. No total, 40% (18/45) demonstraram conhecer por completo o princípio, de modo que informaram práticas que garantem a exatidão dos dados armazenados — por meio de implementação do banco de dados que respeitam as Formas Normais e atualizações pelos próprios usuários — e técnicas que impeçam a manipulação dos mesmos por usuários não autorizados — com autenticação por sessão e validação por *tokens* — (vide Figura 4.6).

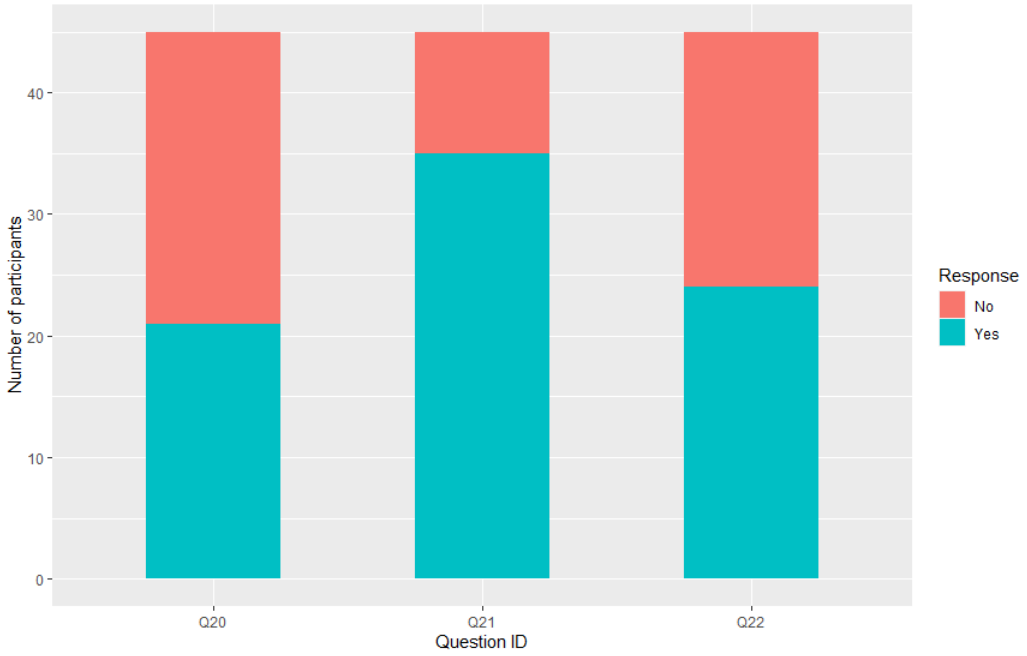

Figura 4.6: Conformidade dos participantes com o princípio de qualidade dos dados.

A maioria dos respondentes, isto é, 44,4% (20/45), ou não sabem garantir a exatidão dos dados ou não conhecem métodos de autenticação, sendo que o maior problema foi o de certificar a exatidão, como segue a transcrição:

> *"É impossível determinar isso devido ao fator humano. É possível aplicar máscaras dentro do cadastro para validar a formatação das informações, mas como todos os dados são inseridos por humanos, ainda permanece o fator da falha."*

Apenas 15,6% (7/45) dos participantes não souberam informar práticas relacionadas ao princípio e, quanto a implementação, pouco mais da metade — 53,3% (24/45) — informou que já havia realizado, e a maioria não obteve dificuldade alguma (vide Tabela

4.8). Dentre as dificuldades citadas, a principal foi respectiva a ferramenta utilizada, que variam desde problemas internos (compreensão da ferramenta e projeto da funcionalidade na mesma) e externos (adequação às mudanças, uma vez que múltiplas pessoas interagem em múltiplos contextos).

Tabela 4.8: Dificuldades de implementação do princípio de qualidade dos dados.

Dificuldade encontrada	#	%
Ferramenta utilizada	6	25
Limitação pela organização	1	4,2
Relacionamento com o usuário	1	4,2
Compreensão da funcionalidade	1	4,2
Sem dificuldades	15	62,5

Dentre a parcela que nunca implementou a funcionalidade — 46,7% (21/45) —, quase todos sinalizaram que o motivo foi a falta de compreensão por completo do princípio, como mostrado na Tabela 4.9, seguido por problemas similares aos encontrados no princípio de livre acesso.

Tabela 4.9: Motivos da falta de implementação do princípio de qualidade dos dados.

Motivo apontado	#	%
Não tenho domínio	18	85,7
Não era um requisito funcional	2	9,5
Não era minha responsabilidade	1	4,8

Para as questões Q23, Q24 e Q25, relativas ao princípio da transparência, uma maior parte de 64,4% (29/45) dos respondentes afirmou não conhecer técnicas específicas de notificação dos usuários sobre as etapas de tratamento dos dados, haja vista Tabela 4.7. A parcela de participantes que apresentou técnicas, de 35,6% (16/45), expressou em massa o interesse dessa comunicação via *e-mail*, inclusive através de serviços automatizados como o *Mautic*.

Ainda sobre o princípio de transparência, foi perguntado aos participantes se consideram importante o registro no sistema de cada operação realizada pelos agentes de tratamento. Uma maioria de 89% dos participantes concordam ou concordam totalmente, 9% nem concordam ou discordam e somente 2% discordam ou discordam totalmente (conforme questão Q24 da Figura 4.1).

A respeito da prévia implementação dessa funcionalidade que reflete o princípio de transparência, somente um terço dos respondentes declarou possuir experiência com registros de *log* e auditoria, de modo que a dificuldade de quase metade foi em definir quais dados são importantes manter em armazenamento (mostrado na Tabela 4.10).

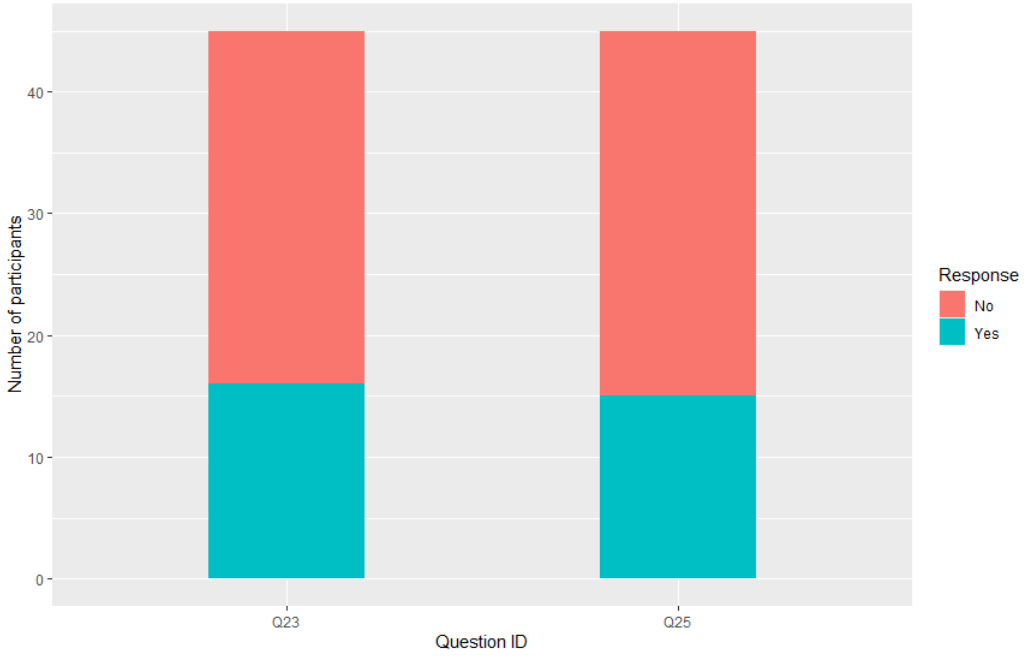

Figura 4.7: Conformidade dos participantes com o princípio de transparência.

Tabela 4.10: Dificuldades de implementação do princípio de transparência.

Dificuldade encontrada	#	%
Volume e separação dos dados	6	40
Limitação pela organização	2	13,3
Sem dificuldades	7	46,7

O dilema abordado pelos participantes deve-se, em grande proporção, acerca da quantidade de dados e o possível impacto no desempenho do sistema. Um participante declarou que, mesmo que essa funcionalidade seja garantida na organização, é por tempo limitado, de modo a impossibilitar a disposição dessas informações para os usuários, como segue a transcrição:

> *"[...] devido ao sistema da empresa, essa informação só ficava disponível por 3 meses. Caso fosse detectado um abuso por algum operador após 3 meses do ato infracional, não teríamos como verificar."*

A fração dos respondentes que nunca implementaram essa função em aplicações, isto é, 66,7% (30/45), informou majoritariamente não haver domínio sobre a funcionalidade, seguido de que não era um requisito funcional ou não era sua respectiva responsabilidade (dispostos na Tabela 4.11).

Tabela 4.11: Motivos da falta de implementação do princípio de transparência.

Motivo apontado	#	%
Não tenho domínio	24	80
Não era um requisito funcional	5	16,7
Não era minha responsabilidade	1	3,3

Sobre a conformidade com o princípio da segurança, referente às questões Q26, Q27, Q28 e Q29, uma maioria de 75,6% (34/45) dos respondentes conhece pelo menos uma técnica para salvaguardar o princípio, mas não todas (haja vista Figura 4.8). Para a garantia da segurança em processos de autenticação e compra, foi citada por quase todos os participantes a encriptação dos dados — adicionada do protocolo *Secure Sockets Layer* (SSL) em determinados casos — e a utilização de dois ou mais fatores na autenticação, como *one-time password* (OTP), *tokens* dinâmicos ou simplesmente verificação via celular ou *e-mail*.

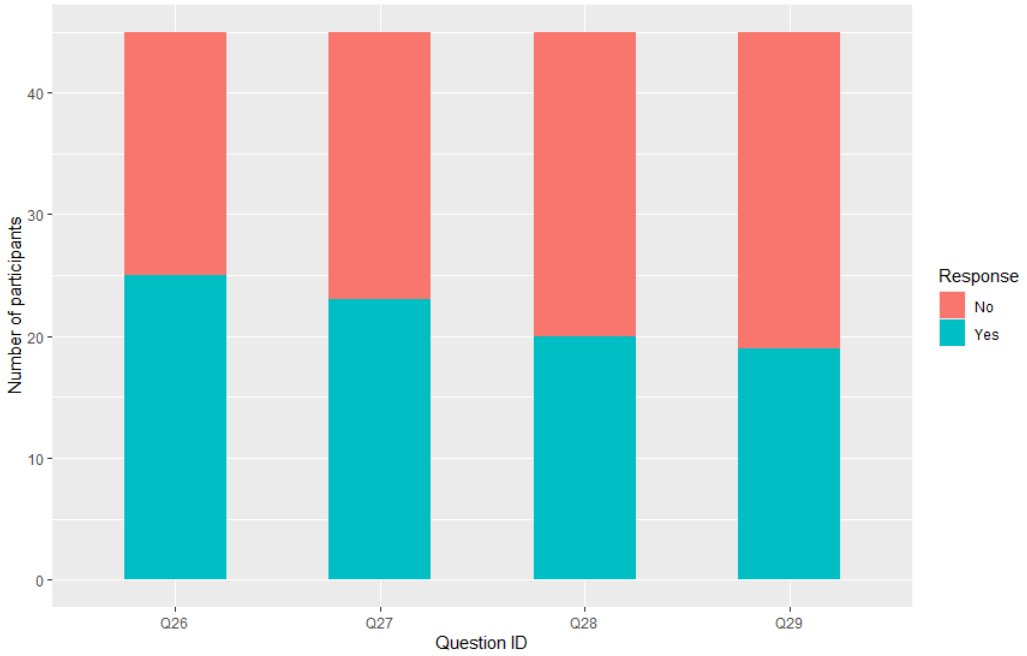

Figura 4.8: Conformidade dos participantes com o princípio de segurança.

Sabe-se que a criptografia, por si só, não impede o vazamento de dados dos usuários do sistema. A fim de evitar essa situação, 51,1% (23/45) dos participantes informaram métodos como a criptografia assimétrica dos dados e a utilização de *hashes* matemáticos, além daqueles voltados para a gestão da organização, como uma verificação adequada da política de segurança da empresa. Uma técnica significativa para garantir a privacidade, mesmo que ocorra um vazamento de informações, é a anonimização (ou despersonificação) dos dados, uma vez que dados identificadores dos usuários são removidos e há garantia do

anonimato dos mesmos. Não obstante, participantes que não souberam informar técnicas afirmaram ser difícil — senão impossível — garantir que não ocorra alguma violação dos dados, como segue a transcrição:

> *"A segurança de um sistema é algo quase impossível de ser impenetrável. O interessante é sempre registrar o caminho dos dados, com algumas labels de segurança, para que, caso haja vazamento, seja fácil identificar onde e como isso ocorreu."*

O impasse em agir reativamente é que há possibilidade real de que o usuário que teve suas informações violadas seja prejudicado. Assim, tanto a organização quanto o usuário poderá acarretar em uma penalidade, como abordado no Capítulo 2 (vide Figura 2.2). Além disso, em relação à LGPD, há infração direta no princípio da prevenção, cujo intuito é prevenir a ocorrência de danos quando do tratamento.

No que diz respeito à experiência de implementação do princípio, uma minoria de 42,2% (19/45) já havia realizado. Esperava-se uma maior parcela, uma vez que o princípio da segurança é o de maior prioridade em implementações recorrentes, como exposto no trabalho de Ribeiro et al. [60]. A maior dificuldade abordada pelos respondentes foi a de compreender o funcionamento do algoritmo e da ferramenta a serem utilizados, além de que poucos citaram impacto no desempenho do sistema.

Tabela 4.12: Dificuldades de implementação do princípio de segurança.

Dificuldade encontrada	#	%
Ferramenta/algoritmo utilizado	8	42,1
Desempenho do sistema afetado	2	10,5
Sem dificuldades	9	47,4

Parte dos usuários afirmaram não ter sido necessário implementar, visto que não eram responsáveis pela área ou já havia sido implementado anteriormente as suas admissões nas respectivas organizações. Dessa forma, não houve motivos externos para que a implementação não fosse realizada.

Haja vista as questões Q30, Q31 e Q32, que tratam da concordância dos participantes com o princípio da prevenção, majoritariamente — 77,8% (35/45), exibido na Figura 4.9 — os respondentes não souberam informar meios de preservar a integridade dos dados nos processos de tratamento. Embora de extrema indispensabilidade em aplicações profissionais [60], dentre todos os princípios da LGPD foi o segundo menos conhecido pelos participantes.

Dentre as técnicas citadas pelos respondentes, estão: redundância, operações com *rollback* — isto é, retorno ao estado prévio à ocorrência de danificação dos dados — e atomicidade das operações. Os participantes também foram questionados sobre uma possível solução frente a um cenário de deterioração dos dados pessoais, em que quase

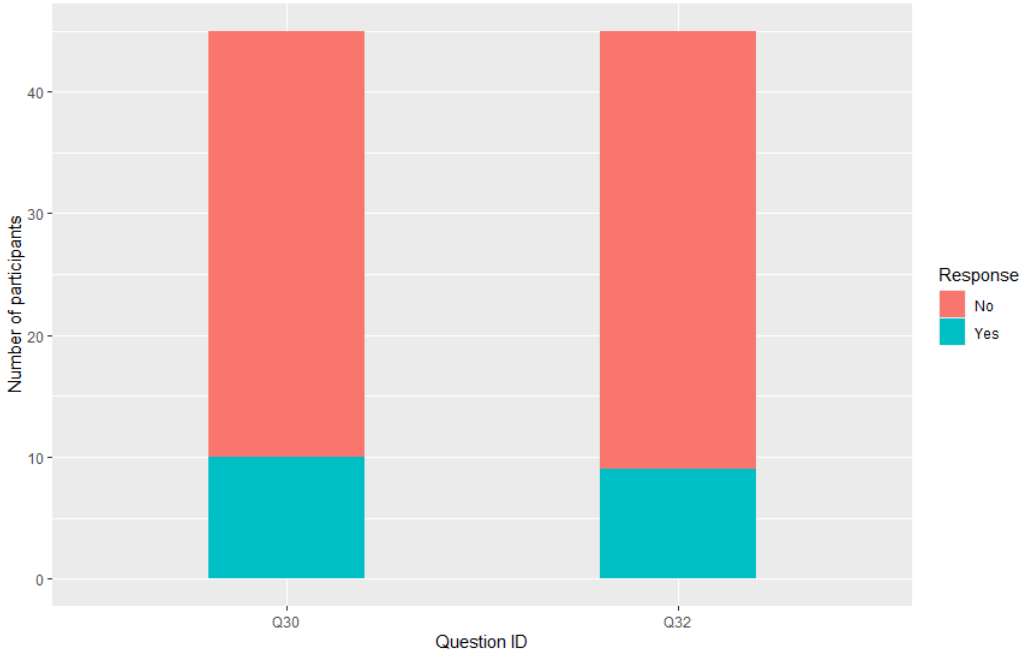

Figura 4.9: Conformidade dos participantes com o princípio de prevenção.

todos os participantes — 95,6% (43/45) — preferem uma implementação preventiva em oposição a uma reativa (exposta na Figura 4.10).

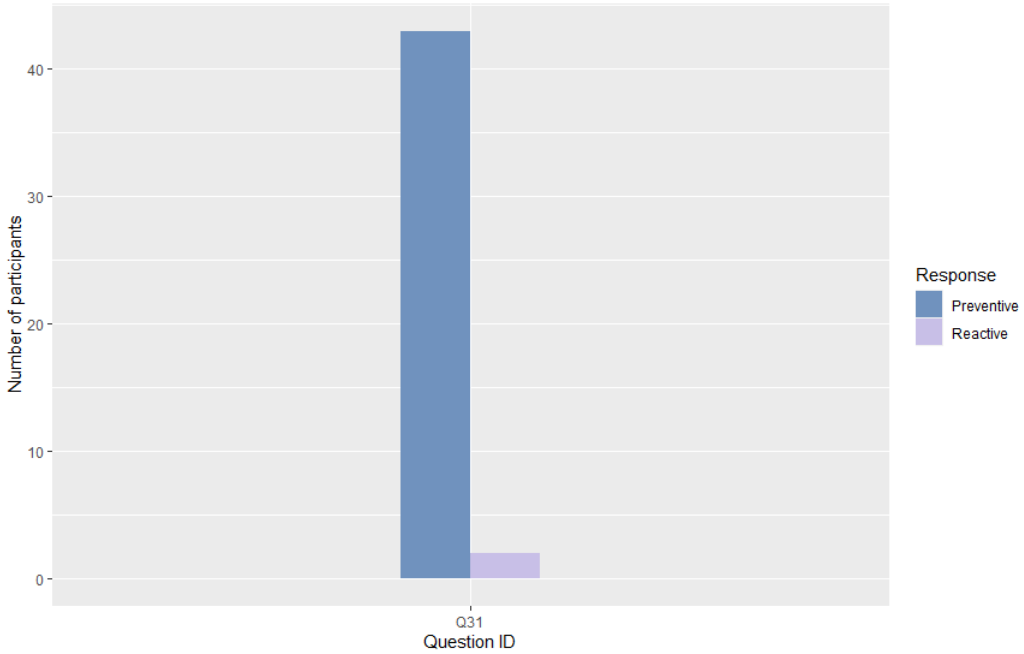

Figura 4.10: Relação de concordância sobre questão do princípio de prevenção

No mesmo cenário, os participantes foram questionados sobre práticas que contenham a funcionalidade de evitar que os dados sejam danificados durante o tratamento dos

dados. Nesse caso, apenas 20% (9/45) já havia implementado, de modo que somente 3 participantes relataram dificuldades, registradas na Tabela 4.13.

Tabela 4.13: Dificuldades de implementação do princípio de prevenção.

Dificuldade encontrada	#	%
Ferramenta utilizada	1	11,1
Compreensão da funcionalidade	1	11,1
Mapeamento das operações	1	11,1
Sem dificuldades	6	66,7

O novo impasse abordado (mapeamento das operações) foi relatado por um único participante e se relaciona pela falta de atomicidade das operações, como segue a transcrição do problema relatado:

> *"As maiores dificuldades estavam ligadas a mapear todas as situações que poderiam levar à danificação de alguma operação e implementação de mecanismos para evitar erros, como por exemplo uma cobrança duplicada ou uma falta de cobrança, porém indicação que ocorreu com sucesso."*

Acerca dos motivos pelo qual não houve implementação da funcionalidade supracitada, a maioria dos participantes relatou não ter a experiência necessária, tal qual relatado na Tabela 4.14. Ainda uma parcela menor de 30% relatou que não era de sua respectiva responsabilidade ou não era um requisito funcional, isto é, os dados tratados não eram cruciais, haja vista a descrição de um dos participantes:

> *"Os dados manipulados não eram críticos."*

Tabela 4.14: Motivos da falta de implementação do princípio de prevenção.

Motivo apontado	#	%
Não tenho domínio	25	69,4
Não era um requisito funcional	7	19,4
Não era minha responsabilidade	4	11,1

Em seguida, relativo ao princípio da não discriminação (questões Q33, Q34, Q35 e Q36), os resultados de conhecimento de técnicas foram não muito superiores em relação ao princípio da prevenção, e os resultados de implementações foram inferiores ao mesmo. Cerca de 6,7% (apenas 3) dos participantes demonstraram conhecer todas as técnicas requisitadas para garantia do princípio.

Além disso, 37,8% (17/45) dos respondentes constataram que conhecem uma ou duas técnicas. Dessa forma, as questões sobre métodos para impedir o tratamento enviesado de dados pessoais (sensíveis ou não) e para contestar os responsáveis em caso de discordância

do tratamento obtiveram respostas proporcionalmente semelhantes. Isso significa que os respondentes apresentaram dificuldade similar em informar técnicas para as três situações abordadas, o que pode ser averiguado na Figura 4.11 (Q33, Q34 e Q35).

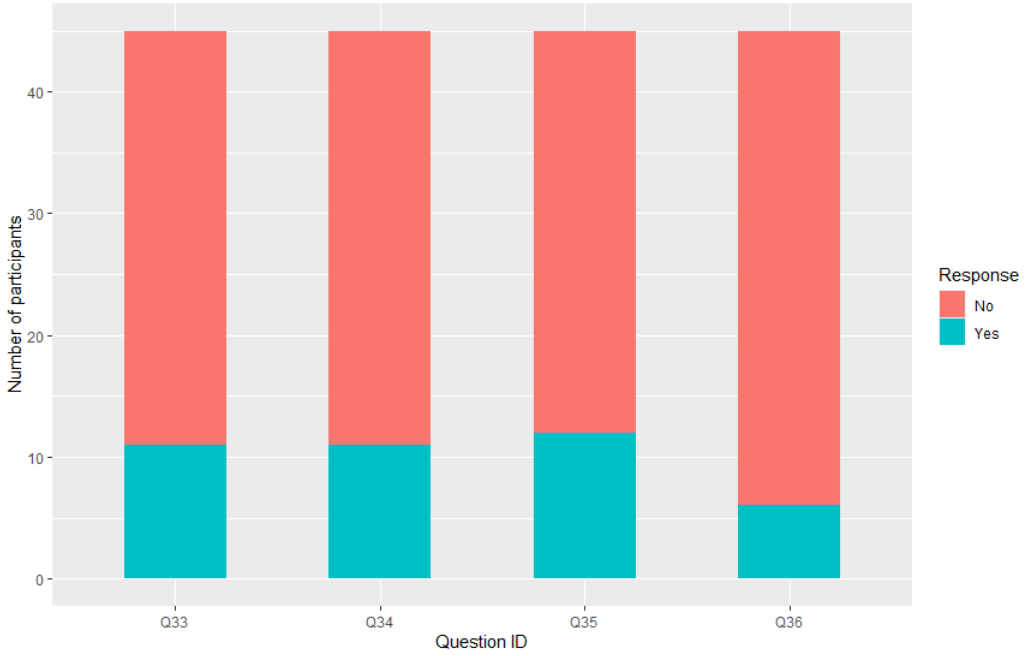

Figura 4.11: Conformidade dos participantes com o princípio de não discriminação.

Dentre os métodos citados pelos respondentes para garantir que o tratamento dos dados pessoais (sensíveis e não sensíveis) não será enviesado, aproximadamente metade informou que é necessário aplicar a técnica de anonimização. Adicionalmente, foi abordado pelos participantes inclusive o porquê da utilização da técnica, seguida de um questionamento, tal qual na transcrição a seguir:

> *"Se você não puder diferenciar os dados de um cliente do outro fica difícil de discriminar, mas ao mesmo tempo fica difícil de auditar. Afinal, se um cliente fraudar, como identificá-lo?"*

Em relação às técnicas que permitam às requisições por parte dos usuários, todos os participantes informaram a necessidade de um canal específico para tal funcionalidade, seja via *e-mail*, formulário ou atendimento via SAC.

Ainda no escopo do princípio da não discriminação, somente 13,3% (6/45) dos respondentes afirmaram já ter implementado a funcionalidade de recorrer aos responsáveis em caso de discordância do tratamento. Ademais, a maioria dos participantes declararam não conhecer tal funcionalidade, tanto como desenvolvedor quanto como usuário. Um único participante apontou uma dificuldade de implementação, que seria na relação entre o responsável e o usuário (deve ficar claro e intuitivo ao usuário o responsável pelo tratamento, para evitar requisições incorretas).

Sobre os motivos da maior parte dos participantes não ter implementado ainda a funcionalidade, primordialmente é a falta de compreensão do princípio, tanto teórico quanto prático. Ainda poucos desenvolvedores comunicaram que não era um requisito funcional ou não era responsável pelo setor, como mostrado na Tabela 4.15.

Tabela 4.15: Motivos da falta de implementação do princípio de não discriminação.

Motivo apontado	#	%
Não tenho domínio	34	87,2
Não era um requisito funcional	3	7,7
Não era minha responsabilidade	2	5,1

O princípio que obteve a menor quantidade relativa de participantes que conhecem todas as técnicas foi o da responsabilização e prestação de contas. Somente 4,4% (2/45) dos respondentes citaram técnicas que garantem a rastreabilidade dos responsáveis pelo tratamento dos dados e que garantem a eficácia do tratamento. O maior problema abordado por quase todos os desenvolvedores — 6,7% (3/45) — em relação a todos os princípios foi o de expor técnicas que possam mensurar a eficácia do tratamento adotado pelos responsáveis. Já 28,9% (13/45) soube informar técnicas que asseguram a rastreabilidade. A proporção de ambas é apresentada na Figura 4.12, além da proporção de profissionais que já implementou uma função de rastreabilidade.

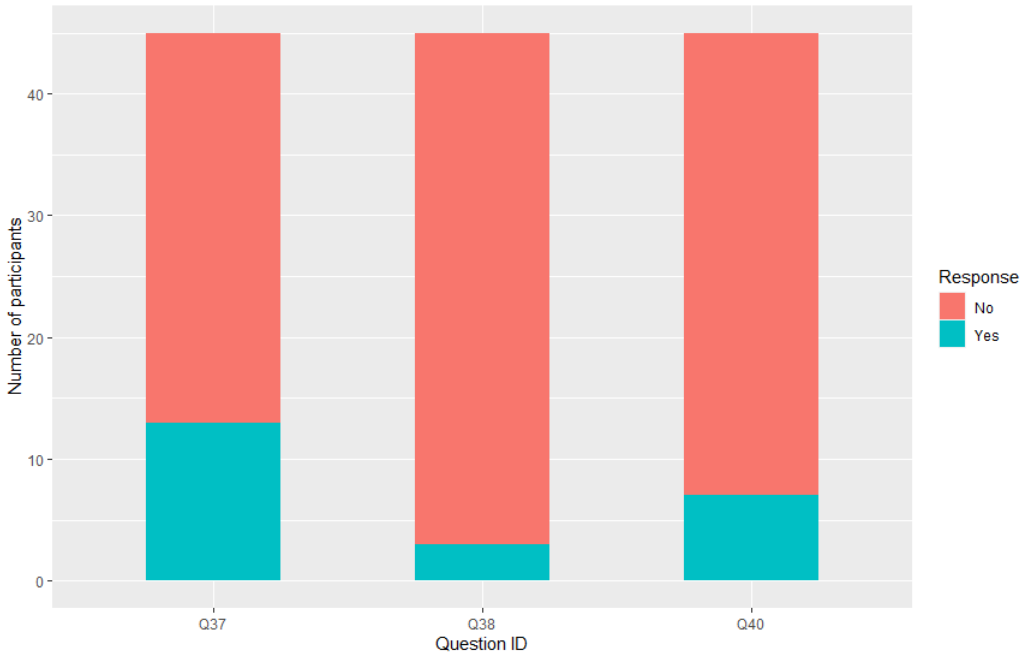

Figura 4.12: Conformidade dos participantes com o princípio de responsabilização e prestação de contas.

Similarmente, os participantes foram questionados se consideram importante manter a rastreabilidade dos responsáveis enquanto durar o processo do tratamento, isto é, para todo o ciclo de vida do dado. 84% concorda ou concorda plenamente, enquanto apenas 2% discorda ou discorda totalmente, conforme questão Q40 da Figura 4.1.

Isso significa que, ainda que a maioria dos respondentes não esteja completamente familiarizada com o princípio de responsabilização e prestação de contas, é inegável que quase todos, aproximadamente 98%, não discorda da relevância de se manter a rastreabilidade. Em contrapartida, devido à falta de familiaridade com o princípio, 15,6% (7/45) já desenvolveu uma funcionalidade que comprometa o responsável com o tratamento.

Sobre as técnicas informadas que dizem respeito à rastreabilidade, quase todos os participantes apontaram registros de auditoria ou *logs* de sistema, com o armazenamento das seguintes informações: responsáveis pelo tratamento, horário do tratamento, dados que acessaram e realizaram as respectivas atividades. Já para

Três respondentes declararam que houve dificuldades (Tabela 4.16), de modo que duas estavam relacionadas à compreensão das operações de tratamento que deveriam ser dispostas aos usuários e uma à ferramenta adotada, isto é, rede *Deep-level transient spectroscopy* (DLTS) com esquema de permissões.

Tabela 4.16: Dificuldades de implementação do princípio de responsabilização e prestação de contas.

Dificuldade encontrada	#	%
Mapeamento das operações	2	28,6
Ferramenta utilizada	1	14,3
Sem dificuldades	4	57,1

A maioria dos participantes declarou nunca ter implementado por falta de familiaridade com o princípio — apresentado na Tabela 4.17 —, sendo que poucos outros informaram que não era um requisito funcional do sistema (inclusive, o custo para implementar tal princípio poderia deixar o sistema obsoleto).

Tabela 4.17: Motivos da falta de implementação do princípio de responsabilização e prestação de contas.

Motivo apontado	#	%
Não tenho domínio	31	81,6
Não era um requisito funcional	6	15,8
Não era minha responsabilidade	1	2,6

Dessarte, após a apresentação das respectivas dificuldades expostas pelos participantes em cada princípio, foi possível esquematizá-los e ordená-los com relação às respostas. A conformidade dos respondentes com a LGPD, no geral, segue o gráfico da Figura 4.13.

Dessa forma, o princípio que os participantes demonstraram maior complexidade no desenvolvimento de suas respostas foi o de responsabilização e prestação de contas, dado que para todas as respectivas questões, uma minoria evidenciou técnicas que podem ser utilizadas para garantia do princípio.

É interessante observar que, no trabalho proposto por Canedo et al. [19], há uma tabela comparativa entre quais princípios da LGPD se relacionam com os princípios da GDPR. Dessa forma, ao se verificar o estudo que motivou o atual trabalho — realizado por Alhazmi et al. [17] —, os maiores empecilhos identificados aos profissionais de software no que diz a GDPR foram os princípios de adequação (equivalente ao de *storage limitation*), de finalidade (equivalente ao de *purpose limitation*) e de qualidade dos dados (equivalente ao de *accuracy*).

No atual trabalho pode-se verificar que os participantes não obtiveram tanta dificuldade em responder questões relacionadas aos princípios de qualidade dos dados e de finalidade, apesar de que o princípio de adequação foi um obstáculo relativo para a maior parcela dos respondentes (mas não foi o regulamento em que os desenvolvedores apresentaram maior dificuldade, vide Figura 4.13).

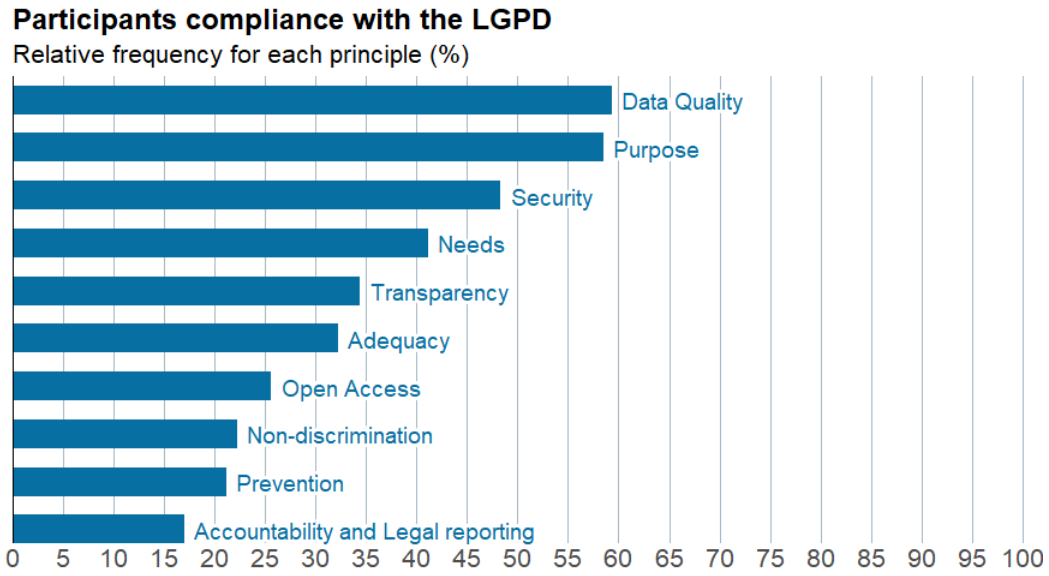

Figura 4.13: Relação de conformidade dos participantes com a LGPD.

4.2 Limitações e Ameaças para Validar o Estudo

Não é possível garantir que todos os artigos, relacionados à aplicação da Lei Geral de Proteção de Dados no contexto de desenvolvimento de software, puderam ser selecio-

nados para desenvolvimento da revisão teórica. Para mitigar essa ameaça, realizou-se as pesquisas nas bibliotecas digitais separadamente, a fim de que a escolha dos artigos pudesse ser mais abrangente.

Uma outra ameaça para a validar o estudo, referente à divulgação do *survey*, foi a realização da mesma de forma manual. Isso significa que o algoritmo utilizado pela plataforma principal de divulgação, o LinkedIn, pode ter sugerido pessoas interconectadas (de formações acadêmicas e localidades semelhantes). Para mitigar, divulgou-se a pesquisa em outros grupos de diferentes plataformas para profissionais da área de tecnologia, mas não é possível garantir que a seleção tenha sido totalmente arbitrária.

Além disso, o tamanho da amostra utilizada foi uma limitação para o estudo. Deve-se ter cautela ao generalizar os resultados obtidos para toda a população brasileira de desenvolvedores, uma vez que foi selecionado apenas um número limitado de participantes. Ademais, a configuração experimental do estudo baseou-se no cenário de um comércio eletrônico, que pode não refletir na atuação profissional de cada um dos participantes e pode ter colaborado com as respostas de profissionais da subárea. Uma limitação relacionada à elaboração do *survey* é que as questões formuladas não abrangem a totalidade de cada princípio, de modo que se buscou apenas averiguar a essência de cada regulamento.

Por fim, uma ameaça relativa às respostas dos questionários é que a pesquisa foi realizada de maneira assíncrona, o que pode ter motivado os respondentes a pesquisarem sobre o assunto, caso não soubessem como responder. Igualmente, os participantes podem não ter concedido a devida atenção, a fim de que finalizassem o *survey* rapidamente. Para mitigar ambos casos, um aviso legal foi redigido no começo do questionário, a fim de informar que a decisão de participar é voluntária e completamente anônima. Espera-se que isso tenha motivado apenas pessoas interessadas em participar da pesquisa.

4.3 Guia Referencial Prático

O objetivo do guia referencial proposto é contribuir para a compreensão dos desenvolvedores de software em relação aos princípios da LGPD. O documento é constituído, inicialmente, pela definição legal de cada princípio exatamente como consta no Art. 6° [14]. A partir disso, busca-se oferecer técnicas de implementação, que garantam que a conformidade com cada princípio seja estabelecida, aos profissionais da área. Por fim, encontra-se uma descrição em grau superior de detalhamento, com exemplos de como poderá fazer uso de tais técnicas.

No que diz respeito às técnicas recomendadas, essas foram selecionadas por dois motivos: citadas frequentemente pelos participantes em resposta às questões do *survey*, o que

significa que uma parcela dos respondentes já possuem familiaridade com o método; ou informadas como efetivas nos estudos propostos na seção de Referencial Teórico.

Já acerca da descrição em um maior grau de detalhamento, houve o intuito de relacionar as técnicas com situações do cotidiano dos desenvolvedores de software. Ademais, buscou-se manter o equilíbrio entre possíveis interesses das organizações e seus usuários, dado que pode ocorrer uma limitação aos profissionais por parte de suas respectivas companhias.

O guia é apresentado nas Figuras 4.14, 4.15 e 4.16, em que cada qual possui cinco princípios, suas descrições legais, técnicas referentes e observações.

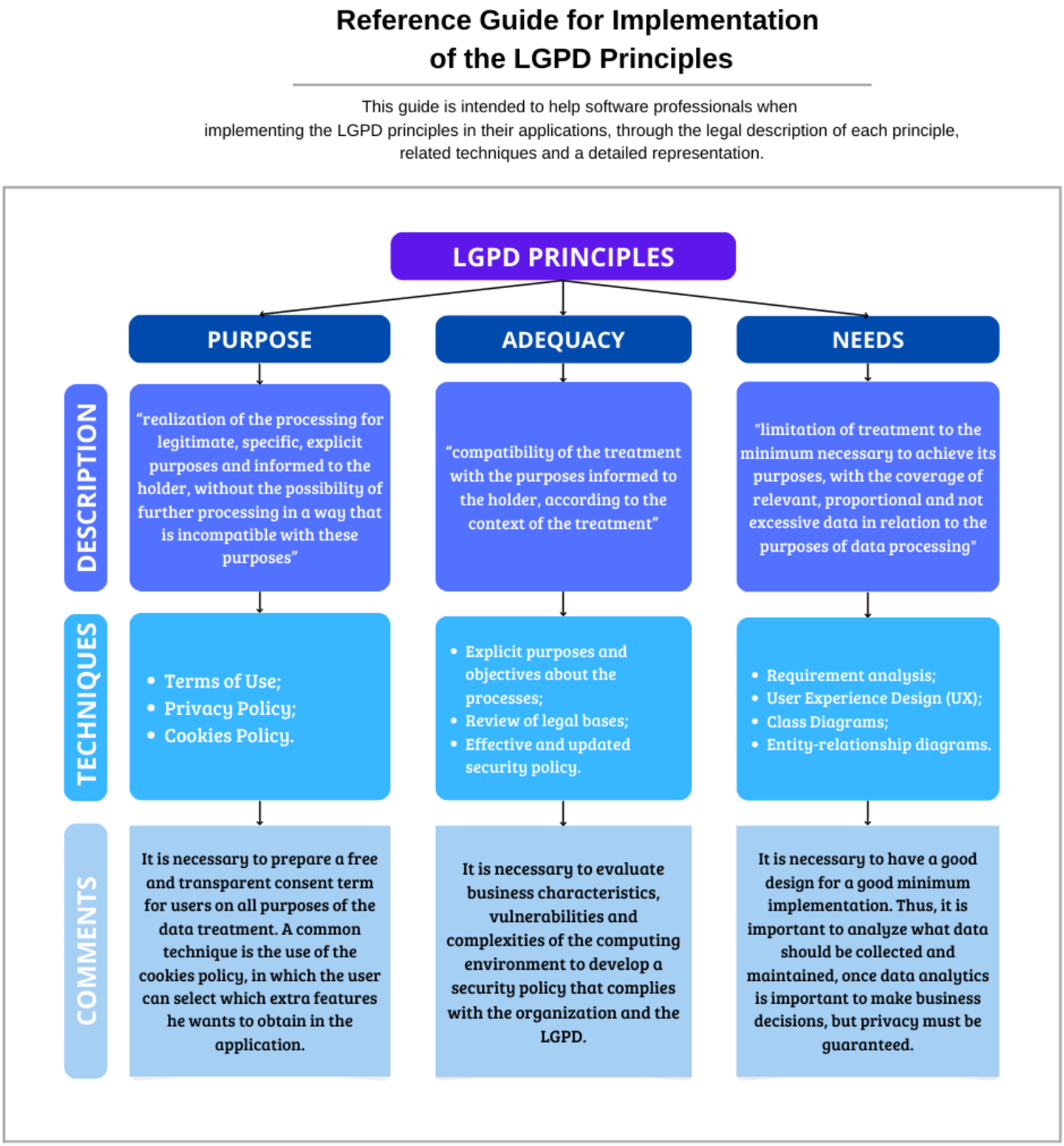

Figura 4.14: Guia Referencial para Implementação LGPD (parte 1).

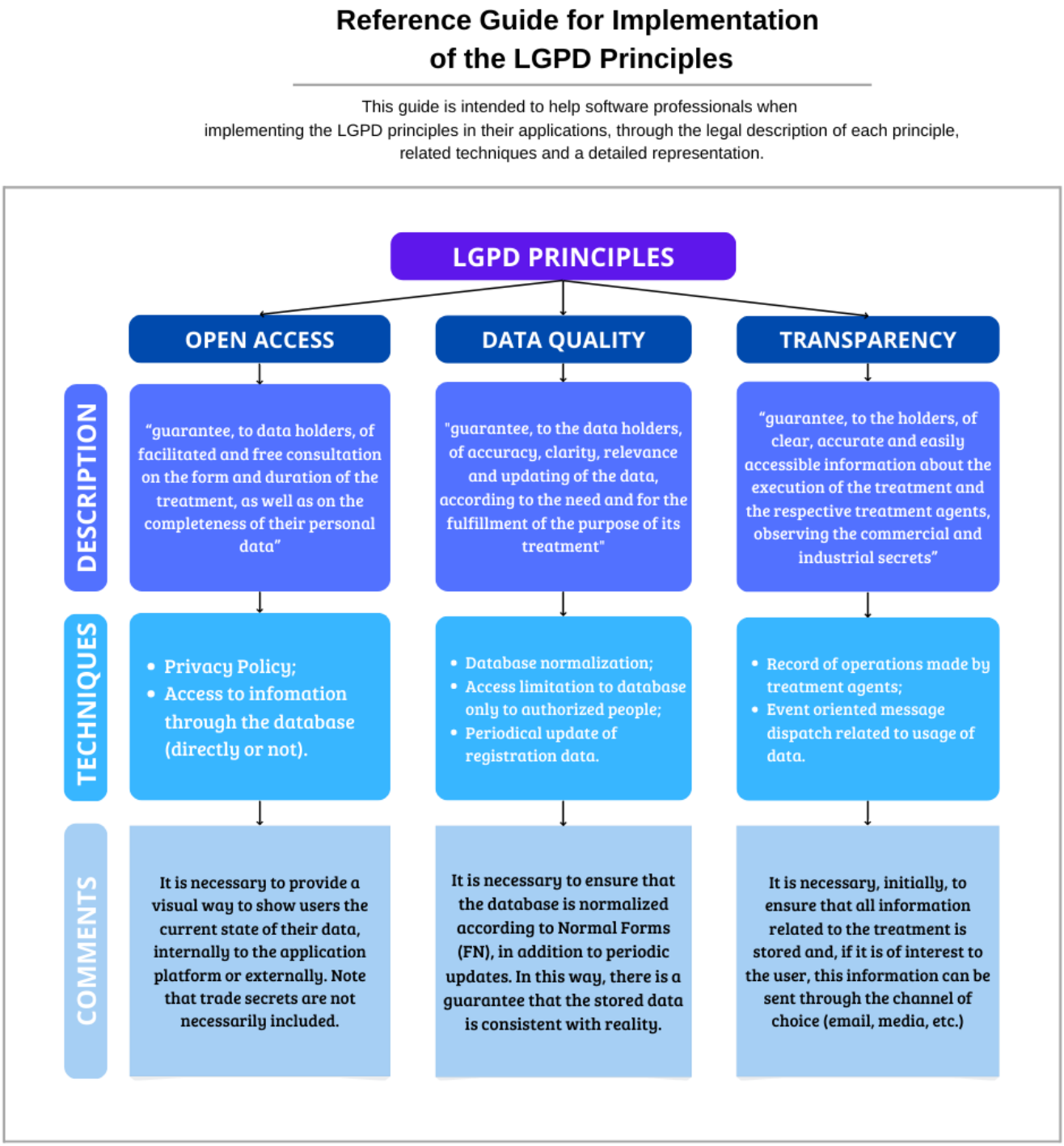

Figura 4.15: Guia Referencial para Implementação LGPD (parte 2).

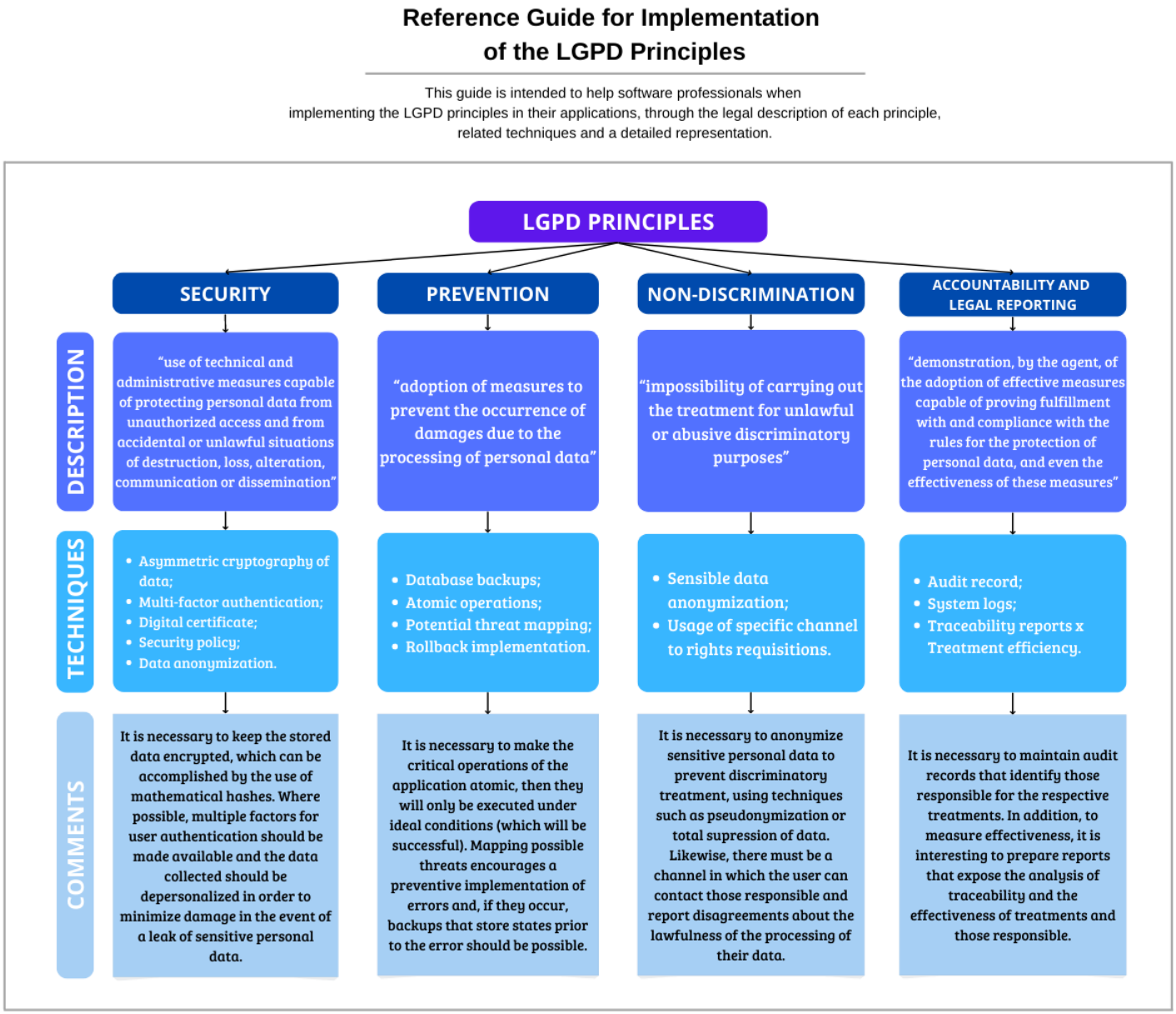

Figura 4.16: Guia Referencial para Implementação LGPD (parte 3).

Capítulo 5

Conclusão

Neste trabalho foi elaborada uma revisão de literatura com o intuito de contextualizar conceitos e práticas relacionadas à garantia da privacidade e da segurança. Os estudos apresentados evidenciam os princípios e limites da privacidade e, no âmbito tecnológico, *frameworks* utilizados, bem como as leis europeia e brasileira de proteção de dados pessoais e as dificuldades apresentadas pelos profissionais de garantia da conformidade com as diretrizes.

A fim de se concretizar o método experimental, houve a criação de um cenário que assimila as funcionalidades de uma aplicação *web* para um comércio eletrônico. Dessa forma, foram elaborados *surveys*, com questionamentos referentes aos princípios da Lei Geral de Proteção de Dados Pessoais (LGPD), para evidenciar as principais dificuldades de implementação dos desenvolvedores e projetistas de software. Por meio da prática de teoria fundamentada foi possível destacar, dentre os questionamentos, os princípios que foram considerados obstáculos pelos profissionais.

Como resultado do trabalho, a maioria dos participantes do *survey* pertenciam à etapa de desenvolvimento de software, isto é, a programação de aplicações, além de que quase metade declarou possuir mais de 3 anos de experiência em seus cargos atuais. Ademais, as respostas do *survey* apontam que 73% dos respondentes acreditavam estar a par das diretrizes da LGPD, todavia nenhum respondente demonstrou conhecer técnicas de implementação para garantia de todos os princípios da lei. A principal dificuldade relatada pelos respondentes foi de que não conheciam algum princípio específico e, dentre os participantes que conheciam, não implementavam pois não possuíam o conhecimento ou material necessário. Para todos os princípios, ocasionalmente foi informado que não era um requisito funcional da aplicação — em exceção o de segurança — ou não era de responsabilidade do participante. Por fim, o princípio em que os profissionais apresentaram maior dificuldade foi o de responsabilização e prestação de contas, em que 83% não conheciam técnicas para garantia total, de modo que mais de 80% não havia sequer

implementado anteriormente.

Em relação aos trabalhos futuros, pode-se experimentar uma maior parcela dos profissionais da área, a fim de que seja conduzida uma pesquisa em uma metodologia quantitativa. Além disso, é interessante um estudo especializado em cada uma das áreas profissionais, visto que possibilita a descoberta de entraves específicos de cada etapa do desenvolvimento de software.

Referências

[1] Lambrechts, Wynand, Saurabh Sinha e Sarah Mosoetsa: *Colonization by algorithms in the fourth industrial revolution*. IEEE Access, 10:11057–11064, 2022. https://doi.org/10.1109/ACCESS.2022.3145236. 1

[2] Kuo, Yong-Hong e Andrew Kusiak: *From data to big data in production research: the past and future trends*. Int. J. Prod. Res., 57(15-16):4828–4853, 2019. https://doi.org/10.1080/00207543.2018.1443230. 1

[3] Johnson, Joseph: *Internet usage worldwide—statistics & facts*. Statista: New York, NY, USA, 2021. https://www.statista.com/statistics/617136/digital-population-worldwide/, acesso em 12/02/2022. 1

[4] Gao, Yuan, Yi Li, Yunchuan Sun, Zhipeng Cai, Liran Ma, Matevz Pustisek e Su Hu: *IEEE access special section: Privacy preservation for large-scale user data in social networks*. IEEE Access, 10:4374–4379, 2022. https://doi.org/10.1109/ACCESS.2020.3036101. 1

[5] Garfinkel, Simson e Gene Spafford: *Web security, Privacy & Commerce*. O'Reilly Media, Inc., 2002. 1

[6] Cheng, Long, Fang Liu e Danfeng Yao: *Enterprise data breach: causes, challenges, prevention, and future directions*. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 7(5):e1211, 2017. 1, 13, 18

[7] Marks, Gene: *A LinkedIn 'Breach' Exposes 92% Of Users—And Other Small Business Tech News*. Forbes, 2021. https://www.forbes.com/sites/quickerbettertech/2021/07/05/a-linkedin-breach-exposes-92-of-usersand-other-small-business-tech-news/?sh=50a7a2b55b33, acesso em 15/03/2022. 1

[8] Perlroth, Nicole: *All 3 Billion Yahoo Accounts Were Affected by 2013 Attack*. The New York Times, 2017. https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html, acesso em 15/03/2022. 1

[9] Collier, Kevin e Jason Abbruzzese: *Twitter breach exposes one of tech's biggest threats: Its own employees*. NBC News, 2020. https://www.nbcnews.com/tech/security/twitter-breach-exposes-one-tech-s-biggest-threats-its-own-n1234076, acesso em 15/03/2022. 1

[10] Daniel, Ellen: *Instagram, Tiktok and Youtube user data left unsecured in data breach.* Verdict, 2020. https://www.verdict.co.uk/instagram-data-breach/, acesso em 15/03/2022. 1

[11] Isaak, Jim e Mina J. Hanna: *User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection.* Computer, 51(8):56–59, 2018. https://doi.org/10.1109/MC.2018.3191268. 1

[12] 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, 25

[13] Alkubaisy, Duaa, Luca Piras, Mohammed Ghazi Al-Obeidallah, Karl Cox e Haralambos Mouratidis: *Confis: A tool for privacy and security analysis and conflict resolution for supporting GDPR compliance through privacy-by-design.* Em Ali, Raian, Hermann Kaindl e Leszek A. Maciaszek (editores): *Proceedings of the 16th International Conference on Evaluation of Novel Approaches to Software Engineering, ENASE 2021, Online Streaming, April 26-27, 2021*, páginas 80–91. SCITEPRESS, 2021. https://doi.org/10.5220/0010406100800091. 2, 3

[14] 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, 21, 22, 23, 24, 28, 30, 31, 32, 58

[15] Brasil: *Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet.* Diário Oficial da República Federativa do Brasil, 2014. http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. 2

[16] *Guia de Elaboração de Inventário de Dados Pessoais*, 2021. https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_inventario_dados_pessoais.pdf, acesso em 22/04/2022. 2, 21, 22

[17] 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. 2, 3, 13, 17, 20, 21, 24, 26, 42, 57

[18] Sakamoto, Liliam Sayuri, Davis Alves, Jair Minoro Abe, Jonatas Santos de Souza, Nilson A. de Souza e Angel Antonio Gonzalez Martinez: *Software optimization for LGPD compliance using Paraconsistent Evidential Annotated Logic Eτ.* Em Watróbski, Jaroslaw, Wojciech Salabun, Carlos Toro, Cecilia Zanni-Merk, Robert J. Howlett e Lakhmi C. Jain (editores): *Knowledge-Based and Intelligent Information & Engineering Systems: Proceedings of the 25th International Conference KES-2021,*

Virtual Event / Szczecin, Poland, 8-10 September 2021, volume 192 de *Procedia Computer Science*, páginas 3049–3059. Elsevier, 2021. https://doi.org/10.1016/j.procs.2021.09.077. 2, 3, 9

[19] 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. 3, 8, 57

[20] Taplin, Steve: *The Future of Software Development in 2022 and Beyond*. Entrepreneur, 2022. https://www.entrepreneur.com/article/403829, acesso em 19/03/2022. 3

[21] Breaux, Travis e Jennifer Moritz: *The 2021 software developer shortage is coming*. Commun. ACM, 64(7):39–41, 2021. https://doi.org/10.1145/3440753, acesso em 19/03/2022. 3

[22] Alhazmi, Abdulrahman e Nalin Asanka Gamagedara Arachchilage: *Why are Developers Struggling to Put GDPR into Practice when Developing privacy-preserving software systems?* CoRR, abs/2008.02987, 2020. https://arxiv.org/abs/2008.02987. 3

[23] 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. 4

[24] Warren, Samuel D e Louis D Brandeis: *Right to privacy*. Harv. L. Rev., 4:193, 1890. 7

[25] Lauterpacht, Hersch: *The universal declaration of human rights*. Brit. YB Int'l L., 25:354, 1948. 7

[26] Brasil: *Constituição da República Federativa do Brasil de 1988*. Congresso Nacional, 1988. http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. 7

[27] Brasil: *Lei nº 10.406, de 10 de janeiro de 2002. Código Civil*. Diário Oficial da República Federativa do Brasil, 2002. http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. 7

[28] Westin, Alan F: *Privacy and Freedom atheneum*. New York, 7:431–453, 1967. 7, 8

[29] Floridi, Luciano: *Information ethics: On the philosophical foundation of computer ethics*. Ethics and information technology, 1(1):33–52, 1999. 8

[30] Mayer-Schönberger, Viktor: *General development of data protection in Europe*. Technology and privacy: The new landscape, páginas 219–242, 1997. 8, 23

[31] 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. 8, 9, 10, 11

[32] HEW, United States Secretary of Health and Human Services: *The Code of Fair Information Practices*. https://archive.epic.org/privacy/hew1973report/c3.htm. 10

[33] OECD: *The OECD Privacy Framework*, 2013. https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf. 11, 14, 16

[34] Klitou, Demetrius: *A solution, but not a panacea for defending privacy: the challenges, criticism and limitations of privacy by design*. Em *Annual Privacy Forum*, páginas 86–110. Springer, 2012. 12

[35] Caiza, Julio C, Jose M Del Alamo, Danny S Guamán e Ángel Jaramillo-Alcázar: *An exploratory experiment on privacy patterns: limitations and possibilities*. Em *Proceedings of the 36th Annual ACM Symposium on Applied Computing*, páginas 1209–1216, 2021. 12

[36] Zhang, Heng, Yuanchao Shu, Peng Cheng e Jiming Chen: *Privacy and performance trade-off in cyber-physical systems*. IEEE Network, 30(2):62–66, 2016. 12

[37] Hoepman, Jaap-Henk: *Privacy design strategies - (extended abstract)*. Em Cuppens-Boulahia, Nora, Frédéric Cuppens, Sushil Jajodia, Anas Abou El Kalam e Thierry Sans (editores): *ICT Systems Security and Privacy Protection - 29th IFIP TC 11 International Conference, SEC 2014, Marrakech, Morocco, June 2-4, 2014. Proceedings*, volume 428 de *IFIP Advances in Information and Communication Technology*, páginas 446–459. Springer, 2014. https://doi.org/10.1007/978-3-642-55415-5_38. 13

[38] Hustinx, Peter: *Privacy by design: delivering the promises*. Identity in the Information Society, 3(2):253–255, 2010. https://doi.org/10.1007/s12394-010-0061-z. 13

[39] Cavoukian, Ann: *Privacy by design*, 2009. 13, 14, 16, 23

[40] Kalloniatis, Christos, Evangelia Kavakli e Stefanos Gritzalis: *Addressing privacy requirements in system design: the pris method*. Requirements Engineering, 13(3):241–255, 2008. 17

[41] Schaar, Peter: *Privacy by design*. Identity in the Information Society, 3(2):267–274, 2010. 17

[42] 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. 17

[43] Brown, Allison J: *"should I Stay or Should I Leave?": Exploring (dis) continued Facebook use after the Cambridge analytica scandal*. Social Media+ Society, 6(1):2056305120913884, 2020. 17

[44] 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 22/04/2022. 18, 19, 20, 24

[45] Hoofnagle, Chris Jay, Bart van der Sloot e Frederik Zuiderveen Borgesius: *The European Union general data protection regulation: what it is and what it means*. Information & Communications Technology Law, 28(1):65–98, 2019. 18

[46] Albrecht, Jan Philipp: *How the GDPR will change the world*. Eur. Data Prot. L. Rev., 2:287, 2016. 18

[47] *Sanções Administrativas: o que muda após 1º de agosto de 2021?*, 2021. https://www.gov.br/anpd/pt-br/assuntos/noticias/sancoes-administrativas-o-que-muda-apos-1o-de-agosto-de-2021, acesso em 22/04/2022. 21

[48] Novakoski, André Luis Mota e Samyra Haydêe Dal Farra Naspolini: *Responsabilidade civil na LGPD: problemas e soluções*. Conpedi Law Review, Florianópolis, 6(1):158–174, 2020. 21

[49] Goswami, Puneet e Suman Madan: *Privacy preserving data publishing and data anonymization approaches: A review*. Em *2017 International Conference on Computing, Communication and Automation (ICCCA)*, páginas 139–142. IEEE, 2017. 22

[50] Okano, Marcelo T, Lamara Ferreira, Henry de Castro dos Santos e Edson L Ursini: *Lgpd o novo desafio para as organizações: Exemplos de frameworks para diagnosticar este novo cenário*. South American Development Society Journal, 7(20):380, 2021. 24

[51] Gheisari, Mehdi, Hamid Esmaeili Najafabadi, Jafar A Alzubi, Jiechao Gao, Guojun Wang, Aaqif Afzaal Abbasi e Aniello Castiglione: *OBPP: An ontology-based framework for privacy-preserving in IoT-based smart city*. Future Generation Computer Systems, 123:1–13, 2021. 24

[52] Cormack, Andrew: *Thinking with gdpr: A guide to better system design*, 2021. 25

[53] 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. 25

[54] Canedo, Edna Dias, Vanessa Coelho Ribeiro, Anderson Jefferson Cerqueira, Rogério Machado Gravina, Renato Camões, Vinicius Eloy dos Reis, Fábio Lúcio Lopes Mendonça e Rafael T. de Sousa: *Evaluating and evolving the compliance to the brazilian general data protection law in a federal government agency*. Em Filipe, Joaquim,

Michał Śmiałek, Alexander Brodsky e Slimane Hammoudi (editores): *Enterprise Information Systems*, páginas 3–27, Cham, 2022. Springer International Publishing, ISBN 978-3-031-08965-7. 25

[55] 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. 25, 43, 46

[56] 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. 26

[57] Chun Tie, Ylona, Melanie Birks e Karen Francis: *Grounded theory research: A design framework for novice researchers.* SAGE open medicine, 7:2050312118822927, 2019. 27

[58] Meng, Na, Stefan Nagy, Danfeng Yao, Wenjie Zhuang e Gustavo Arango Argoty: *Secure coding practices in java: Challenges and vulnerabilities.* Em *Proceedings of the 40th International Conference on Software Engineering*, páginas 372–383, 2018. 27

[59] Hoda, Rashina: *Decoding Grounded Theory for Software Engineering.* Em *43rd IEEE/ACM International Conference on Software Engineering: Companion Proceedings, ICSE Companion 2021, Madrid, Spain, May 25-28, 2021*, páginas 326–327. IEEE, 2021. https://doi.org/10.1109/ICSE-Companion52605.2021.00139. 37

[60] 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. 51