Uma taxonomia para requisitos de privacidade e sua aplicação no Open Banking Brasil

Sâmmara Éllen Renner Ferrão[1][0000−0002−8372−0358] and Edna Dias Canedo[1,2][0000−0002−2159−339X]

[1] Departamento de Engenharia Elétrica (ENE), Mestrado Profissional em Engenharia Elétrica,
Universidade de Brasília (UnB), Brasília–DF, Brasil sammaraellen@gmail.com
[2] Departamento de Ciência da Computação, Universidade de Brasília (UnB), Brasília, DF, Brasil, ednacanedo@unb.br

Abstract. A preocupação com a privacidade de dados é vem se destacando ao longo dos anos em diversos países. No Brasil a Lei Geral de Proteção de Dados (LGPD) foi publicada em agosto de 2018, entrando em vigor em 2020 porém, algumas dificuldades ainda são enfrentadas pelos profissionais de TIC na adequação dos mecanismos tecnológicos, por parte das organizações. Assim, este trabalho propõe uma taxonomia de requisitos de privacidade baseada na LGPD e na ISO/IEC 29100 com o objetivo de apoiar as equipes de desenvolvimento de software no alcance da conformidade com os princípios da LGPD. A aplicação prática da taxonomia proposta foi realizada no processo de solicitação de consentimento e no termo e condições de consentimento do projeto Open Banking de três bancos no Brasil. A taxonomia de requisitos proposta é composta por 129 requisitos de privacidade divididos em 10 categorias e 5 contextos. A aplicação prática da taxonomia resultou em um percentual satisfatório de aderência aos requisitos de privacidade demonstrando a possibilidade de apoio as equipes de desenvolvimento de software na busca pela adequação à LGPD especificamente no âmbito dos requisitos de privacidade.

Keywords: Requisitos de Privacidade · Taxonomia · LGPD · Open Banking.

1 Introdução

A preocupação dos usuários com a proteção de seus dados é algo que vem se desenvolvendo desde a entrada em vigor da Lei Geral de Proteção de Dados (LGPD) [30]. Os eventos recentes de vazamento de dados [3, 16, 1, 17] tornam ainda mais evidente a necessidade de garantir a proteção dos dados pessoais. Isso especialmente no cenário brasileiro em que apenas 20% das empresas brasileiras estabeleceram processos de comunicação sobre possíveis vazamentos de dados e apenas 23% realizam gerenciamento de incidentes para lidar de forma eficaz com possíveis vazamentos de dados [20].

Já no âmbito do desenvolvimento de software os requisitos não funcionais (RNF), podem descrever como o sistema deve se comportar [9] e a negligência tanto para documentá-los quanto a possibilidade de não considerá-los parece ser um dos maiores problemas relacionados a esse tipo de requisito [9, 12, 14, 28]. Alguns autores destacaram que os RNF comumente são descritos de maneira incompleta, [11, 2, 18]. Como requisitos de privacidade são geralmente categorizados como requisitos não funcionais, eles podem compartilhar dos mesmos desafios. Em sua natureza, os requisitos de privacidade podem ser utilizados para registros de requisitos fundamentados em bases legais, esse contexto dificulta a elicitação dos requisitos uma vez que essa atividade geralmente é exercida por analistas de requisitos/sistemas que não possuem experiência na interpretação de normas legais [7, 15, 25, 4]. Nesse sentido, identifica-se a necessidade de uma abordagem prática em relação a elicitação de requisitos de privacidade no contexto das legislações e *frameworks* de segurança e privacidade. Para atender este desafio de uma abordagem prática, neste trabalho propõe-se uma taxonomia de requisitos de privacidade no contexto da LGPD. Alguns autores abordaram sobre taxonomias de requisitos de privacidade [31, 24, 26, 8], mas apenas o trabalho de Sangaroonsilp et al. [31] se assemelha com esta pesquisa por ter proposto uma taxonomia de requisitos de privacidade baseada na GPDR, essa proposição foi utilizada como inspiração para criação desta taxonomia baseada na LGPD.

Nesse contexto, esse artigo apresenta a proposta de uma taxonomia de requisitos de privacidade baseada na LGPD e na ISO/IEC 29100 para apoiar as equipes de desenvolvimento de software na conformidade com os princípios da LGPD. Com essa taxonomia os analistas estarão de posse de uma lista de requisitos de privacidade dos quais seus sistemas precisam estar em aderentes para alcançar a conformidade com a LGPD. Assim, as principais contribuições desse trabalho são: i) uma taxonomia de requisitos de privacidade que pode ser utilizada como um *guideline* pelos profissionais de Tecnologia da Informação e Comunicação (TIC) durante a elicitação e especificação de requisitos; e ii) um formulário para avaliar a adequação à LGPD dos sistemas já desenvolvidos, permitindo a identificação dos pontos de não conformidade para regularização. As duas principais contribuições visam o alcance conformidade com a LGPD.

2 Referencial Teórico

A Lei Geral de Proteção de Dados (LGPD) [30] é a lei brasileira para proteção de dados pessoais e foi inspirada na GDPR [29]. Sua publicação aconteceu em agosto de 2018 com entrada em vigor em agosto de 2020. Com isso o Brasil passou a compor um grupo de mais da metade de países (66% dos países no mundo possuem alguma legislação relacionada a proteção e privacidade de dados) que possuem leis para a proteção dos dados pessoais, segundo dados de setembro de 2020 da organização intergovernamental ligada à ONU *United Nations Conference on Trade and Development* (UNCTAD) [33].

A LGPD estabelece que o processamento de dados poderá ser executado pelas instituições de direto privado desde que seja solicitado ao titular do dado um

consentimento para tal. Esse consentimento deverá indicar uma finalidade específica para tanto não são permitidas autorizações genéricas e vícios de consentimento também não são permitidos [30]. Informações como essas demonstram a importância de desenvolvimento de iniciativas que proporcionem às instituições formas para estarem aderentes à LGPD.

Sobre a privacidade de dados, Canedo et al. [15] registram que ela compreende os dados do usuário, criados por ele mesmo ou terceiros e sua utilização por meio de observações, análises, entre outros, por indivíduos. Finkelstein, M. e Finkelstein, C. [21] consideram que a evolução tecnológica é um marco na história da privacidade. A preocupação com a privacidade também aumentou ao longo do tempo, principalmente pela rápida evolução no processamento de dados [32].

A definição de requisitos de privacidade, de acordo com Webster et al. [34], é o requisito capaz de registrar os objetivos de privacidade e as medidas associadas a esses objetivos para um determinado sistema. Por essa natureza subjetiva, os requisitos de privacidade são geralmente categorizados como Requisitos não funcionais e com isso acabam compartilhando dos mesmos desafios em seu processo de elicitação destacados por [9, 12, 14, 28, 11, 2, 18, 10].

Alves e Neves [1] estabeleceram uma análise empírica de questões sobre privacidade para elaboração de proposta de padrões de privacidade seguindo um guia de pesquisa qualitativa e *Grounded theory*. Essa análise foi realizada a partir de entrevistas semi estruturadas (27 Questões) com profissionais com mais 10 anos de experiência e que acumulam cargos de gestão em uma organização pública. Foram feitas as análises nas transcrições das entrevistas que geraram como resultado alguns pontos de perspectivas que podem auxiliar os profissionais de TI na elicitação de requisitos de privacidade e a partir disso foram gerados padrões de privacidade aplicados pontualmente no Sistema piloto analisado. Este trabalho se difere do trabalho de Alves e Neves por propor uma taxonomia de requisitos de privacidade enquanto Alves e Neves abordaram apenas a análise empírica das dificuldades de elicitação dos requisitos de privacidade.

Em 2015, Meis et al. [27] desenvolveram uma taxonomia de requisitos de transparência com base na ISO/IEC 29.000 [23] e no rascunho do Regulamento de Proteção de Dados da UE, uma vez que o GDPR[29] ainda não havia sido publicada. Essa taxonomia teve como objetivo fornecer aos engenheiros de software um método para identificar os requisitos de transparência. Eles analisaram a descrição dos princípios de privacidade na ISO e as formulações do projeto do regulamento. Os autores encontraram trinta requisitos de transparência e sua validação foi executada comparando outras taxonomias encontradas em uma Revisão de Literatura. O projeto de Meis et al. [27] se difere deste projeto estar relacionado com requisitos de transparência e não com requisitos de privacidade. Também se difere por ser baseado em um rascunho da GDPR, já este trabalho a LGPD, legislação brasileira vigente e aprovada em 2018.

Sangaroonsilpet al. [31] desenvolveram uma taxonomia de requisitos de privacidade baseada na GDPR e ISO/IEC 29100. Para o desenvolvimento desta taxonomia foram utilizadas as técnicas GBRAM e teoria fundamentada com um método de 3 passos para obtenção dos requisitos de privacidade que re-

sultaram em uma lista de sete categorias com um total de 149 requisitos de privacidade. Todos os requisitos identificados a partir da ISO/IEC 29100 estavam contemplados pelos encontrados na GDPR. Essa taxonomia foi utilizada como inspiração para o desenvolvimento desta proposta de taxonomia baseada na LGPD e ISO/IEC 29100 porém elas se diferem principalmente por esta última estar inserida no contexto brasileiro de legislação e por ter gerado uma quantidade diferentes de requisitos além de uma estrutura diferente de representação hierárquica dos requisitos.

3 Desenvolvimento da Taxonomia Proposta

Essa pesquisa foi conduzida utilizando multi-metodologias. A elaboração da taxonomia foi baseada no processo de análise de conteúdo *Goal-Based Requirements Analysis Method* (GBRAM) [6, 5] e na Teoria Fundamentada dos Dados [22] (*Grounded Theory*) (Figura 1). Em seguida o processo de replicação dos passos estabelecidos por Sangaroonsilp et al. [31] foram executados, porém sobre o contexto da LGPD. Em seguida a taxonomia foi aplicada em um cenário real, para avaliação de aderência à LGPD e por últimos a verificação dos resultados foi executada para análise desta taxonomia (Figura 1).

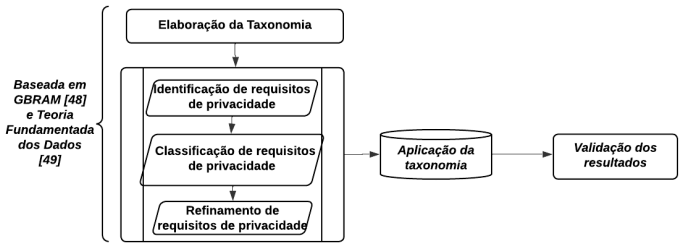

Fig. 1: Metodologia de Pesquisa

A proposição da taxonomia de requisitos de privacidade foi baseada nos princípios definidos no processo de análise de conteúdo adaptado do *Goal-Based Requirements Analysis Method* (GBRAM) [5], método utilizado para identificar, elaborar, refinar e organizar objetivos para a especificação de requisitos. Esse método foi utilizado por Antón e Earp [6] no desenvolvimento da taxonomia de requisitos para redução de vulnerabilidades em websites e na taxonomia de requisitos de privacidade proposta por Sangaroonsilp et al. [31] baseada na GDPR e ISO/IEC 29100, processos utilizados como referência para este trabalho.

Para o desenvolvimento desta taxonomia a regulamentação de privacidade foi utilizada e um *framework* amplamente conhecido e estabelecido em relação à privacidade de dados que daqui em diante, quando referenciados em conjuntos, serão endereçados como base taxonômica: a legislação brasileira de proteção de

dados pessoais, a LGPD [30] e a ISO/IEC 29100 [23]. O método para o desenvolvimento desta taxonomia é divido em 3 passos principais, estabelecidos a partir das técnicas do GBRAM e *Grounded Theory* [5, 31]: TP1 **Identificação dos requisitos de privacidade** responsável por analisar a legislação e o *framework* em busca dos requisitos de privacidade para composição da taxonomia. É um passo executado a partir de uma análise crítica dos documentos para composição dos itens. TP2 **Classificação dos requisitos de privacidade** Elaboração da classificação dos requisitos em categorias, de acordo com a lista de objetivos de privacidade. TP3 **Refinamento dos requisitos de privacidade** remoção dos possíveis itens duplicados e ajuste de possíveis inconsistências considerando duas fontes de identificação para os requisitos.

3.1 TP1 - Identificação de Requisitos de Privacidade

Para execução desta etapa foram analisados todos os 28 artigos da LGPD nos quais as declarações foram encontradas. Na ISO/IEC 29100 foram analisadas 58 declarações dentro dos princípios de privacidade estabelecidos por essa norma. Foram ao todo identificados 112 requisitos de privacidade a partir da LGPD e 57 requisitos de privacidade a partir da ISO/IEC 29100. As instruções sobre cada um dos passos e o processo executado são:

TP1.a Identificação de ações: Para cada afirmação nas regulações, são procuradas as ações perguntando "Qual ação deve ser fornecida com base nesta afirmação?". **TP1.b Determinação das partes envolvidas/afetadas:** Com a identificação da ação, é necessário em seguida identificar o objeto dessa ação perguntando "Quem está envolvido/afetado por essa afirmação?". **TP1.c Ponderação do resultado esperado:** Este passo especifica o resultado esperado que pode ser alcançado para atender à privacidade e aos direitos do usuário, perguntando "O que deve ser alcançado com base na ação dessa declaração?". **TP1.d Estruturação em um padrão de requisito:** O requisito de privacidade derivado é codificado no formato de verbo de ação, seguido pelo objeto e objetivo.

Exemplos de aplicação da TP1 : A análise das declarações destacadas pode começar com a execução da seção TP1.a ou pela seção TP1.b. Nesta exemplificação, será iniciado pelo passo TP1.c com a identificação das ações nas sentenças destacadas da LGPD. Para o primeiro exemplo, analisou-se a declaração: *Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais.* **TP1.a:** Nela é identificado que o controlador de dados tem por obrigação indicar um encarregado para o tratamento de dados pessoais. A ação necessária nesta declaração é a **indicação** por parte do controlador, o verbo de ação utilizado então será o **INDICAR**. **TP1.c**: tem-se que o envolvido nesta declaração é o **controlador**, que é o ator que possui uma obrigação. **TP1.c**: verifica-se que o objetivo da declaração é a **indicação do encarregado pelo tratamento de dados pessoais. TP1.d**: Com a estruturação, o requisito fica da seguinte forma: *RLGPD069 - INDICAR o encarregado pelo tratamento de dados pessoais.*

3.2 TP2 - Classificação dos requisitos de privacidade

Nesta etapa, foram definidas as categorias da Taxonomia e executada a classificação dos 169 requisitos obtidos na fase anterior. Esse processo foi divido entre a **Definição dos objetivos de cada meta de privacidade** e *a Consideração do resultado esperado* de um requisito. Para tal foram considerados os 10 princípios definidos na LGPD e os 9 princípios ISO/IEC 29100. Numa análise comparativa o princípio da *não discriminação* da LGPD não está incluído em nenhum dos princípios da ISO, justificando a diferença de quantidade de princípios entre a base taxonômica. Princípios como *Consentimento e escolha* e *Legitimidade e especificação do propósito* da ISO são cobertos pelo princípio de *Finalidade* da lei. Além desses, os princípios *Minimização de dados* e *Limitação de uso, retenção e divulgação* da ISO são cobertos pelo princípio *Necessidade* da LGPD. Com isso, foi identificado que todos os princípios da ISO/IEC 29100 são cobertos pelos princípios da LGPD. Considerando os pontos expostos, essa taxonomia se utilizará dos princípios da LGPD para a criação de suas categorias.

A definição das categorias está disponível na seção II do pacote de reprodução disponibilizado em [19]. Durante o processo de criação das categorias de requisitos para a taxonomia foi verificada a necessidade de criar uma classificação adicional dada a abrangência da LGPD [30] que contempla vários âmbitos da engenharia de software como processos e governança sobre o aspecto de proteção dos direitos pessoais. Isso pois foram identificados contextos além dos sistêmicos. Esses contextos serão definidos adicionalmente à categoria para que os analistas de sistemas consigam classificar as necessidades dentro de sua instituição para a completa adequação à LGPD. São eles: **C.1 Software**: identifica requisitos de privacidade que podem ser implementados em softwares. Ou seja, requisitos de sistema que podem ser validados por regras de negócio em requisitos de privacidade; **C.2 Estudos e pesquisa**: são requisitos de privacidade processuais que determinam como órgãos de pesquisa devem seguir para o tratamento de dados; **C.3 Governança**: identifica os requisitos que não necessariamente podem ser atendidos por sistemas, mas que precisam ser implementados pela organização, com controles e mecanismos de governança para a garantia dos princípios da LGPD; **C.4 Gestão Pública**: os requisitos que são obrigatórios para órgãos de natureza pública, que precisam ser implementados pela organização para garantir a aderência à legislação principalmente para o tratamento de dados sem a necessidade de consentimento, resguardados pelo direito da natureza dessas instituições; e **C.5 Infraestrutura**: requisitos sobre o processo de transferência internacional de dados com terceiros além processos e controles de armazenamento de dados.

Os requisitos de privacidade podem estar relacionados a uma categoria e também a um contexto. Os contextos podem se repetir pelas categorias. A categoria ainda é o agrupador principal dessa taxonomia por refletir os princípios da LGPD. Na Figura 2 são apresentados os relacionamentos identificados entre categorias e contextos para os requisitos de privacidade elicitados nesta taxonomia. As linhas os relacionamentos entre as categorias e os contextos. Por exemplo, o contexto Software se relaciona com todas as categorias enquanto o contexto

Gestão Pública se relaciona apenas com as categorias de Finalidade, Necessidade e qualidade de dados.

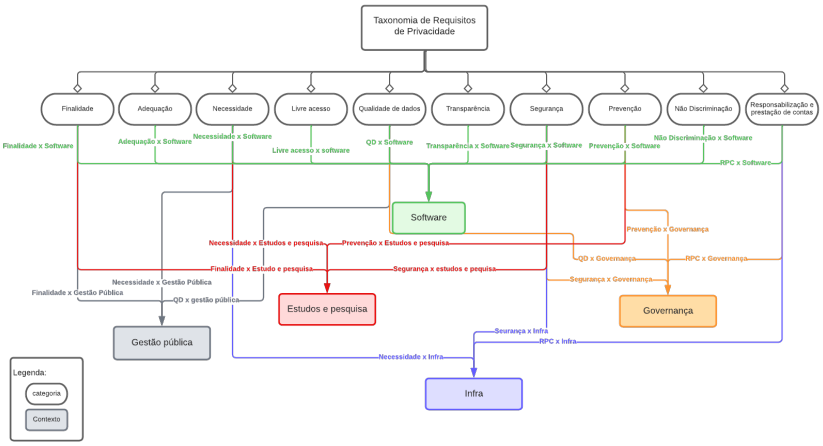

Fig. 2: Taxonomia de requisitos de Privacidade proposta, fonte: Própria

A seguir são apresentados os passos para identificação da categoria e taxonomia para os requisitos de privacidade.

Exemplos de aplicação da TP2 Exemplificando a classificação do requisito gerado no exemplo de aplicação de TP1 - LGPD, é necessário considerar o resultado esperado com esse requisito. O objetivo desse requisito é indicar o encarregado pelo tratamento de dados ao titular dos dados, podendo assim ser categorizado no objetivo **P.6 Transparência**. Por se tratar de algo que não necessariamente será registrado/controlado por sistemas e sim por processos de governança, ele se classifica no contexto de **C.3 Governança**. Os requisitos ainda podem estar duplicados entre si, o que será analisado na próxima etapa.

3.3 TP3 - Refinamento dos requisitos de privacidade

Para o refinamento foram avaliados os 169 requisitos obtidos a partir da base taxonômica (LGPD e ISO/IEC 29100), que podem ter semelhanças ou podem ser redundantes entre si. Com a classificação dos requisitos em categorias ocorreu a identificação dos requisitos semelhantes, que foram adequados para uma versão única e os duplicados foram excluídos. Com o processo de refinamento 27 requisitos foram unificados entre si enquanto 17 requisitos foram identificados como duplicados, 3 requisitos obtidos da ISO/IEC e 3 requisitos obtidos da LGPD foram excluídos. A taxonomia de requisitos de privacidade é composta por 129 requisitos que estão classificados em 10 categorias e 5 contextos e foi disponibilizada no pacote de reprodução [19].

3.4 Aplicação da Taxonomia de Requisitos de Privacidade no Open Banking Brasil

Por estar relacionado com o compartilhamento de dados e ser fundamento na LGPD, o projeto *Open Banking* torna-se um projeto promissor para avaliação da adequação a taxonomia de requisitos de privacidade elaborada neste trabalho. Com isso, foi elaborado um formulário para avaliação da aderência dos processos de compartilhamento de dados dos três maiores bancos do país. Os nomes reais dos bancos foram omitidos e serão referenciados aqui como Banco A, Banco B e Banco C. O formulário foi denominado Formulário de Avaliação de Aderência a taxonomia (FAAT). Nele foram listados os requisitos de privacidade com opções para indicar a aplicação do requisito em relação a instituição financeira avaliada, a partir dos dados coletados. O formulário e o material utilizado para análise estão disponíveis no pacote de reprodução em [19].

4 Resultados da aplicação da Taxonomia Proposta

Analisando os resultados o Banco A, tem-se que 61.54% dos requisitos foram identificados como aplicados, enquanto 32.69% foram considerados parcialmente aplicados e 5.77% foram considerados não aplicados. Para o Banco B, o alcance de 51.92% dos requisitos considerados atendidos parcialmente, enquanto 40.38% foram considerados aplicados e 7.69% foram considerados não aplicados. Por fim, para o Banco C, registra-se que 71.15% dos requisitos de privacidade foram considerados aplicados - Sim - no contexto da Instituição Financeira (IF) em questão, 26.92% foram considerados parcialmente aplicados e apenas 1.92% foram considerados não aplicados. A visão geral do resultado da aderência das instituições a taxonomia é apresentada na Tabela 1.

Table 1: Percentual de adequação à Taxonomia proposta

Banco	**Aplicação dos requisitos de privacidade**					
	Sim		**Parcialmente**		**Não**	
	Percentual	Número	Percentual	Número	Percentual	Número
Banco A	61.54%	32	32.69%	17	5.77%	3
Banco B	40.38%	21	51.92%	27	7.69%	4
Banco C	71.15%	37	26.92%	14	1.92%	1

A seguir são descritos os resultados de acordo com as categorias da taxonomia apresentando apenas os itens identificados como não aplicados ou parcialmente aplicados. **P.1 Finalidade** - Para o **Banco A**, 5 requisitos foram identificados como não ou parcialmente aplicados. Os quais são: RQ001, RQ004, RQ006 e RQ008. O RQ001 foi considerado como aplicado parcialmente por a instituição não permitir a edição do escopo de dados compartilhados e por permitir apenas

dois tipos de prazo de compartilhamento, não se atentando a forma livre e específica prevista para este requisito. O RQ004 tive a aplicação considerada como parcial por não haver a determinação do período de tratamento por parte da IF, apenas do período de compartilhamento. O RQ006 teve a aplicação identificada como parcial pois não foi identificada página pública sobre os procedimentos para revogação de consentimento. No entanto, no Termos e Condições (T&C), há seção específica sobre o processo de revogação mas ainda assim não há determinação dos procedimentos. Para finalizar a análise da aplicabilidade dos requisitos atendidos parcialmente, para o RQ008 a finalidade é definida como *oferecer soluções mais aderentes ao seu perfil de forma segura e sigilosa* porém a instituição não permite a alteração dos tipos de dados compartilhados (Dados cadastrais, dados de contas, etc.). Por fim, no contexto de Gestão Pública, o requisito RQ021 foi considerado não atendido por não ter sido identificada a menção à possibilidade de requerer informações por organismos de defesa do consumidor no T&C e na página de privacidade da IF.

Para o **Banco B**, o RQ001 foi identificado como atendido de forma parcial, pois permite apenas quatro tipos de prazo de compartilhamento, não se atentando a **forma livre e específica do requisito**. Já o requisito RQ002 foi identificado como não aplicado pois não é apresentada a finalidade do tratamento de dados no fluxo de compartilhamento de dados apesar de no item 7 da T&C afirmar que os **dados serão utilizados para as finalidades indicadas no consentimento**. O requisito RQ004 foi considerado como atendido de maneira parcial visto que não há estipulação do período de tratamento, apenas do período de compartilhamento apesar de na página de Termos e Condições haver a informação de **que o prazo pelo qual o Banco B mantém os Dados Pessoais coletados depende do propósito e da natureza do tratamento dos dados**. O requisito RQ006 também foi considerado atendido de maneira parcial, pois a partir da página pública de Termos e Condições citada no T&C é identificada a página de Privacidade da instituição que discorre-se sobre o canal para revogação, porém não há detalhes dos procedimentos necessários. O requisito RQ008, RQ014 e RQ015 tiveram o status de atendido parcialmente, em razão da finalidade não estar prevista no momento do compartilhamento, não sendo possível avaliar se os dados são compatíveis com a finalidade. O requisito RQ009, foi considerado atendido parcialmente, dado que apesar de não haver a finalidade no momento do compartilhamento, há no item 4 do T&C que a declaração de que a instituição *preserva o direito de tratar seus dados*, em consonância com os limites da LGPD. Para o Banco B, por fim, o RQ021 foi considerado como não implementado pois não foi identificada menção à possibilidade de requerer informações por parte dos organismos de defesa do consumidor no T&C e na página de privacidade da IF.

Para o **Banco C**, o requisito RQ004 foi considerado atendido de maneira parcial, posto que não há estipulação do período de tratamento, apenas do período de compartilhamento e por fim o RQ021 foi considerado como não implementado, uma vez que não foi identificada menção à possibilidade de requerer informações

por organismos de defesa do consumidor no T&C e na página de privacidade da IF.

P.3 Necessidade - Para o **Banco A** e **Banco C**, os 6 requisitos RQ042, RQ044, RQ045, RQ046, RQ047 e RQ048 desta categoria, todos do contexto de infraestrutura, foram considerados como atendidos parcialmente, pois, para o primeiro banco a página de política de usos e privacidade, referenciada no T&C, consta que o processo de transferência é feito conforme a LGPD porém não há evidências para comprovar a aplicação. Para o segundo, o disposto na página de Privacidade constante no T&C não faz menção sobre o processo de transferência o que pode indicar que a instituição não o faz ou não contemplou a situação em sua política de privacidade. Para o **Banco B**, 5 foram considerados como atendidos parcialmente, sendo eles RQ042, RQ045, RQ046, RQ047 e RQ048, pois a partir do endereço de Termos de uso disponível no T&C, foi encontrado o endereço da página de Privacidade da IF que discorre sobre a transferência internacional de dados estar de acordo com a LGPD porém não é possível comprovar com evidências a partir das informações utilizadas nesse trabalho. O requisito RQ044 foi considerado como não implementado pois apesar de a partir do endereço de Termos de uso disponível no T&C, ser encontrado no endereço da página de Privacidade que discorre sobre a transferência internacional de dados estar de acordo com a LGPD, no T&C a leitura dos termos demonstra ser opcional.

P.4 Livre Acesso - Para o **Banco A**, **Banco B** e **Banco C** os RQ049 e RQ050 foram considerados como atendidos parcialmente pois apesar de não estarem diretamente disponíveis no processo de consentimento o T&C das IFs menciona na página de Termos de Uso do primeiro banco que contém uma seção "seus dados, seus direitos". Para a segunda IF o T&C menciona de forma abstrata a página Termos de Uso que contém uma seção "Seus direitos" que explica sobre os direitos e como exercê-los. E para o terceiro, apesar de não estar diretamente disponível no processo de consentimento o T&C menciona a página Privacidade com uma seção "seus direitos" referente ao acesso aos dados.

P.5 Qualidade dos Dados - O RQ052, do contexto de software, foi considerado como atendido parcialmente, para as IFs **Banco A**, **Banco B** e **Banco C**, pois apesar de não estar diretamente disponível no processo de consentimento o T&C menciona a página de Termos de uso do primeiro banco contém uma seção "seus dados, seus direitos". Para o segundo, o T&C menciona de forma abstrata a página de Termos de Uso com a seção "Seus direitos" que explica sobre os direitos e como exercê-los. E para o terceiro, porque apesar de não estar diretamente disponível no processo de consentimento o T&C menciona a página de Privacidade com a seção "seus direitos" referente ao acesso aos dados.

P.6 Transparência - Para o **Banco A**, o RQ069 foi considerado como atendido parcialmente pois apesar de o T&C mencionar a página Política de Usos que faz referência ao processo de exclusão, não há muitas instruções que permitam o entendimento por parte do usuário. Para o **Banco B**, 5 requisitos foram considerados como aplicados parcialmente sendo que os requisitos RQ060, RQ063, RQ068 e RQ069 receberam esse status pois apesar de não estarem diretamente

disponíveis no processo de consentimento e de não haver menção no T&C sobre o como exercer os direitos, o T&C menciona de forma abstrata a página de Termos de Uso que contém uma seção "Seus direitos" explicando sobre os direitos e como exercê-los. Já requisito RQ070, também considerado atendido de maneira parcial, em seu T&C menciona de forma abstrata a página de Termos de Uso e nela há a seção *10. ENCARREGADO DE PROTEÇÃO DE DADOS*, porém não há indicação do nome do encarregado, apenas um e-mail institucional para acioná-lo. Para o **Banco C**, os requisitos RQ060 e RQ069 foram considerados atendidos de maneira parcial. O primeiro pelo fato de que é informado na página de Privacidade da IF sobre a possibilidade das solicitações, porém o prazo de 15 dias não é fornecido nessa página e há uma justificativa prévia para um possível atraso. Já o segundo requisito, pois apesar de o T&C mencionar a página de Privacidade da IF com referência a exclusão, não há muitas instruções que permitam o entendimento por parte do usuário.

P.7 Segurança - O RQ084 foi considerado como atendimento parcialmente por todas as IFs (**Banco A, Banco B e Banco C**), pois alguns controles estão registrados pelos bancos em seus respectivos sites de privacidade, porém não é possível avaliar apenas com as informações públicas disponíveis se a aplicabilidade do requisito é completa.

P.10 Responsabilização e Prestação de Contas - Para o **Banco A**, 2 requisitos foram considerados como não aplicados e 2 foram considerado aplicados de forma parcial, os requisitos RQ094 e RQ104 foram considerados não implementados - Não - pois durante a análise não foi identificada seção sobre os tipos de dados pessoais coletados na página de Termos de Uso a qual o T&C se refere. O requisito RQ111 foi considerado atendido parcialmente pois não foi identificada seção relativa a anonimização, apenas sobre a correção. Enquanto para o RQ129 o status parcial foi atribuído pois a garantia de sua aplicação não é avaliável, entretanto, a IF declara que segue os procedimentos, conforme disposto na página de Políticas de uso e privacidade. Para o **Banco B**, os requisitos RQ104, RQ105, RQ106, RQ107, RQ108 foram considerados como atendidos parcialmente pois há menção da anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade porém não há explicação dos procedimentos na página de termos de uso da IF. Enquanto o RQ129, também atendido de maneira parcial, difere em sua avaliação, pois a garantia não é avaliável porém a IF declara que segue os procedimentos na página de termos de uso. Ainda para o **Banco B**, o requisito RQ094 foi considerado como não implementado em razão de não ter sido identificada seção sobre os tipos de dados pessoais coletados nas páginas de termos de uso disponível no T&C e na página de privacidade da IF. Por fim, o **Banco C**, o requisito RQ129 foi considerado atendido de maneira parcial, pois, a garantia não é avaliável, porém a IF declara que segue os procedimentos na página Privacidade.

4.1 Discussão dos Resultados

A taxonomia de requisitos de privacidade baseada na LGPD e ISO/IEC 29000 proposta nesse trabalho foi baseada no processo utilizado por Sangaroonsilp et

al. [31] que segue o *Goal-Based Requirements Analysis Method* (GBRAM) [5] e a *Grounded Theory*. Sua elaboração derivou 10 categorias e 5 contextos de aplicação dos requisitos e 129 requisitos de privacidade. A aplicação do Formulário de Avaliação de Aderência à Taxonomia (FAAT) resultou em 71.15% de aderência à taxonomia para o Banco C, enquanto o Banco A de 61.54%, e por fim o Banco B teve 40.38%. A baixa aderência do Banco B pode se dar pela ausência da finalidade no processo de consentimento, já que muitos requisitos se baseiam na existência da finalidade no processo de consentimento. Como a aplicabilidade geral desse banco foi a menor, na aplicação de forma parcial foi maior para essa instituição apresentando 51.92% dos requisitos de privacidade, seguida do Banco A, que teve a segunda maior aderência, ficando assim com 32.69% dos requisitos de privacidade com aplicabilidade parcial e por fim o Banco C com 26.92%. Esses resultados podem indicar que as instituições financeiras estão de forma geral mais próximas do que distantes da aderência a LGPD no processo de *Open Banking*. Trabalhos anteriores executados sob a perspectiva dos funcionários indicaram que as instituições ainda estavam iniciando a aplicação da LGPD [20]. Os resultados obtidos nesse trabalho indicam maior aderência aos requisitos de privacidade obtidos na LGPD para o projeto do *Open Banking*, o que pode ter acontecido por este projeto ter sido definido após a publicação da LGPD e durante sua entrada em vigor (2020), além de ser um projeto regulado pelo Banco Central, instituição com poder de supervisão [13].

5 Conclusão

Esse artigo teve como objetivo preencher uma lacuna na literatura sob o aspecto de taxonomias de requisito de privacidade com a criação da taxonomia que resultou em 129 requisitos de privacidade classificados em 10 categorias e 5 contextos de aplicação sob a perspectiva da legislação brasileira de proteção de dados pessoais. A aplicação da taxonomia no projeto de *Open Banking* de três instituições financeiras (IF) demonstrou que a instituição com menor aderência registrou um percentual 40% de conformidade com a LGPD a partir da aplicação do Formulário de Avaliação de Aderência à Taxonomia (FAAT) enquanto a IF com maior aderência teve um percentual 71%. Os resultados demonstram que a taxonomia pode apoiar as equipes de desenvolvimento com a verificação de que essas instituições apresentaram maior aderência aos requisitos de privacidade de forma geral em comparação à pesquisas executadas anteriormente sob a perspectiva de funcionários [20]. Como trabalhos futuros, espera-se poder aplicar a taxonomia de requisitos de privacidade em um estudo de caso supervisionado com o apoio de uma equipe de desenvolvimento e negócio para a avaliação de métricas e aplicação de medidas descritivas possibilitando avaliar a completude do requisitos de privacidade dessa taxonomia.

References

1. Alves, C., Neves, M.: Especificação de Requisitos de Privacidade em Conformidade com a LGPD: Resultados de um Estudo de Caso. In: Cruz, Maria Lencastre Pin-

heiro de Menezes (UPE, B., Hadad, Graciela Dora Susana (UNO, A., Marques, Johnny Cardoso (ITA, B. (eds.) Anais do WER21 - Workshop em Engenharia de Requisitos. Editora PUC-Rio, Brasília, DF (2021)
2. Ameller, D., Ayala, C., Cabot, J., Franch, X.: How do software architects consider non-functional requirements: An exploratory study. In: 2012 20th IEEE International Requirements Engineering Conference, RE 2012 - Proceedings (2012)
3. ANPD: Anpd está apurando no caso do vazamento de dados de mais de 220 milhões de pessoas (2021), https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-esta-apurando-no-caso-do-vazamento-de-dados-de-mais-de-220-milhoes-de-pessoas, último acesso em 16 de agosto de 2021.
4. Anthonysamy, P., Rashid, A., Chitchyan, R.: Privacy requirements: Present & future. In: 39th IEEE/ACM International Conference on Software Engineering: Software Engineering in Society Track, ICSE-SEIS 2017, Bueons Aires, Argentina, May 20-28, 2017. pp. 13–22. IEEE Computer Society (2017)
5. Anton, A.I.: Goal-based requirements analysis. In: Proceedings of the IEEE International Conference on Requirements Engineering (1996)
6. Antón, A.I., Earp, J.B.: A requirements taxonomy for reducing Web site privacy vulnerabilities. Requirements Engineering **9**(3), 169–185 (2004)
7. Ayala-Rivera, V., Pasquale, L.: The Grace Period Has Ended: An Approach to Operationalize GDPR Requirements. In: IEEE 26th International Requirements Engineering Conference (RE). pp. 136–146 (2018)
8. Barker, K., Askari, M., Banerjee, M., Ghazinour, K., MacKas, B., Majedi, M., Pun, S., Williams, A.: A data privacy taxonomy. Lecture Notes in Computer Science **5588 LNCS**, 42–54 (2009)
9. Behutiye, W., Karhapää, P., Costal, D., Oivo, M., Franch, X.: Non-functional requirements documentation in agile software development: Challenges and solution proposal. Lecture Notes in Computer Science **10611 LNCS**(December), 515–522 (2017)
10. Berntsson Svensson, R., Gorschek, T., Regnell, B.: Quality requirements in practice: An interview study in requirements engineering for embedded systems. In: Lecture Notes in Computer Science. vol. 5512 LNCS (2009)
11. Borg, A., Yong, A., Carlshamre, P., Sandahl, K.: The Bad Conscience of Requirements Engineering : An Investigation in Real-World Treatment of Non-Functional Requirements. In: Proceedings of the 3rd Conference on Software Engineering Research and Practice in Sweden (SERPS'03) (2003)
12. Cao, L., Ramesh, B.: Agile requirements engineering practices: An empirical study. IEEE Software **25**(1) (2008)
13. Central, B., Nacional, C.M.: Resolução conjunta n. 1, de 4 de maio de 2020
14. De Lucia, A., Qusef, A.: Requirements engineering in agile software development. Journal of Emerging Technologies in Web Intelligence **2**(3) (2010)
15. Dias Canedo, E., Toffano Seidel Calazans, A., Toffano Seidel Masson, E., Teixeira Costa, P.H., Lima, F.: Perceptions of ict practitioners regarding software privacy. Entropy **22**(4) (2020)
16. EBC: Procon de sp notifica empresas de telefonia sobre vazamentos de dados. (2021), https://agenciabrasil.ebc.com.br/justica/noticia/2021-02/procon-de-sp-notifica-empresas-de-telefonia-sobre-vazamentos-de-dados, último acesso em 16 de agosto de 2021.
17. EBC: Sites e aplicativo do ministério da saúde sofrem ataque cibernético (2021), https://agenciabrasil.ebc.com.br/saude/noticia/2021-12/sites-e-aplicativo-do-ministerio-da-saude-sofrem-ataque-cibernetico, último acesso 15 de janeiro de 2022.

18. Eckhardt, J., Vogelsang, A., Fernández, D.M.: Are non-functional requirements really non-functional? an investigation of non-functional requirements in practice. In: Proceedings - International Conference on Software Engineering. vol. 14-22-May-2016 (2016)
19. Ferrao, S., Canedo, E.: Uma taxonomia para requisitos de privacidade e sua aplicacao no open banking brasil - pacote de reprodução (Mar 2022). https://doi.org/10.5281/zenodo.6391815
20. Ferrao, S.E.R., Carvalho, A.P., Canedo, E.D., Mota, A.P.B., Costa, P.H.T., Cerqueira, A.J.: Diagnostic of data processing by brazilian organizations—a low compliance issue. Information **12**(4) (2021)
21. Finkelstein, M., Finkelstein, C.: Privacidade e lei geral de proteção de dados pessoais privacy and general personal data protection law. Revista de Direito Brasileira **23**, 284–301 (2020)
22. Glaser, B.G., Strauss, A.L.: Discovery of grounded theory: Strategies for qualitative research. Aldine Transaction (2017)
23. ISO/IEC: Iso/iec 29100:2011 information technology - security techniques - privacy framework (2011)
24. Kanwal, T., Anjum, A., Khan, A.: Privacy preservation in e-health cloud: taxonomy, privacy requirements, feasibility analysis, and opportunities. Clust. Comput. **24**(1), 293–317 (2021)
25. Maia Peixoto, M.: A Privacy Requirements Specification Method for Agile Software Development Based on Exploratory Studies. Ph.D. thesis, Universidade Federal de Pernambuco (2021)
26. Massey, A.K., Antón, A.I.: A requirements-based comparison of privacy taxonomies. In: First International Workshop on Requirements Engineering and Law, RELAW. pp. 1–5. IEEE Computer Society (2008)
27. Meis, R., Wirtz, R., Heisel, M.: A taxonomy of requirements for the privacy goal transparency. In: Fischer-Hübner, S., Lambrinoudakis, C., López, J. (eds.) Trust, Privacy and Security in Digital Business - 12th International Conference, TrustBus 2015, Valencia, Spain, September 1-2, 2015, Proceedings. Lecture Notes in Computer Science, vol. 9264, pp. 195–209. Springer (2015)
28. Paech, B., Kerlow, D.: Non-Functional Requirements Engineering - Quality is essential. In: Proceedings of the 10th International Working Conference on Requirements Engineering: Foundation for Software Quality (REFSQ'04) (2004)
29. Parliament, E., European Union, C.o.: General Data Protection Regulation (GDPR) (2016)
30. da República, P.: Lei nº 13.709, Lei Geral de Proteção de Dados (lgpd) (8 2018), `http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm`
31. Sangaroonsilp, P., Dam, H.K., Choetkiertikul, M., Ragkhitwetsagul, C., Ghose, A.: A taxonomy for mining and classifying privacy requirements in issue reports. CoRR **abs/2101.01298** (2021), `https://arxiv.org/abs/2101.01298`
32. Schreiber, A.: Right to Privacy and Personal Data Protection in Brazilian Law. Springer International Publishing, Cham (2020). https://doi.org/10.1007/978-3-030-28049-9_2
33. UNCTAD: Data protection and privacy legislation worldwide (2020), `https://unctad.org/page/data-protection-and-privacy-legislation-worldwide`, acessado em 13 de outubro de 2021
34. Webster, I., Ivanova, V., Cysneiros, L.M.: Reusable knowledge for achieving privacy: A canadian health information technologies perspective. WER 2005 - 8th Workshop on Requirements Engineering, Workshop em Engenharia de Requisitos pp. 112–122 (2005)