Especificação de Requisitos de Privacidade em Conformidade com a LGPD: Resultados de um Estudo de Caso

Carina Alves, Moisés Neves

Centro de Informática – CIn
Universidade Federal de Pernambuco – UFPE
Recife, Brasil
cfa@cin.ufpe.br, mnc3@cin.ufpe.br

Resumo. A Lei Geral de Proteção de Dados (LGPD) visa proteger os dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, e que pode impor sanções severas pelo seu não cumprimento. Grande parte das organizações ainda não está preparada e precisa implementar várias medidas para garantir que seus sistemas cumpram a conformidade imposta pela lei. No entanto, a legislação vigente é considerada de difícil entendimento para os profissionais de TI. Estes profissionais enfrentam dificuldades para extrair e operacionalizar requisitos legais e de privacidade. Este artigo apresenta um estudo de caso realizado em uma organização do poder judiciário para entender os principais desafios enfrentados por analistas de requisitos para especificar requisitos de privacidade em conformidade com a LGPD. Como contribuição empírica, discutimos o ponto de vista dos analistas em relação às seguintes categorias: conceitos de privacidade, processo de conformidade, obstáculos na conformidade, *tradeoff* entre privacidade e transparência, rotina de trabalho. A partir das percepções dos participantes do estudo de caso, elaboramos uma proposta baseada em padrões de privacidade. A abordagem proposta foi utilizada para especificar requisitos de privacidade de um sistema de software da organização estudada.

Keywords. Requisitos de privacidade, Lei Geral de Proteção de Dados (LGPD), Padrões de Privacidade, Estudo de Caso.

1 Introdução

Recentemente, inúmeros casos de vazamento de dados foram reportados na mídia. Como exemplo destacarmos o caso em que o Ministério Público do Distrito Federal e Território acusa a empresa de telefonia Vivo de vender indevidamente dados de 73 milhões de usuários, principalmente dados de geolocalização para comercializar publicidade [1]. Outro caso, que foi considerado um dos maiores vazamentos no país, revelou dados pessoais de cerca de 223 milhões brasileiros, sendo expostos dados biométricos, faixa salarial, informações sobre *score* de crédito de consumidores, dados de imposto de renda, perfis de redes sociais e fotografias [2]. Estas situações reforçam a

fragilidade dos sistemas de software em relação a aspectos de privacidade. A privacidade tornou-se uma das principais preocupações no desenvolvimento de software, principalmente devido às incidências sobre a exploração não autorizada de dados, uso indevido de informações armazenadas em aplicativos de mídias sociais e divulgação de informações pessoais para terceiros sem o consentimento dos titulares [3].

Os sistemas e os serviços de software contemporâneos exigem uma conectividade entre indivíduos e entidades corporativas, sejam elas públicas ou privadas, que resultam em atividades de coletar, processar ou divulgar regularmente grandes volumes de dados. É importante salientar que a falta de conformidade com políticas de privacidade pode causar consequências sérias com possíveis danos individuais e sociais. [4] Os dados dos sistemas de software geralmente revelam uma grande quantidade de informações pessoais e que podem ser utilizados para outra finalidade que não seja a demanda de origem. A divulgação de tais informações de forma não autorizada gera inúmeros problemas de privacidade para as organizações.

Como forma de proteger a privacidade de usuários, diversos países elaboraram legislações para governar o uso de dados pessoais, tais como, a *General Data Protection Regulation* (GDPR) na União Europeia e Lei Geral de Proteção de Dados (LGPD) no Brasil. Em particular, a LGPD trata aspectos de privacidade de dados se valendo do princípio da finalidade, pois exige que o tratamento de dados tenha propósitos legítimos, específicos, explícitos e informados ao titular sem a possibilidade posterior de forma incompatível com as finalidades. Apesar dos avanços na legislação a fim de garantir a privacidade de dados dos usuários, o desenvolvimento de sistemas de software em conformidade com tais leis ainda enfrenta diversos desafios. Em particular, vários autores reforçam a necessidade de especificar privacidade durante as fases iniciais do desenvolvimento, ou seja, durante a fase de engenharia de requisitos [5,6,7,8].

Este artigo apresenta um estudo de caso realizado em uma organização pública. A organização estudada visa inserir novas práticas para especificar requisitos de privacidade em seu processo de Engenharia de Requisitos (ER). O estudo de caso apresenta resultados de entrevistas realizadas com cinco analistas de requisitos da organização. As entrevistas revelaram os desafios enfrentados por estes profissionais para especificar requisitos de privacidade em conformidade com a LGPD. Em particular, eles relataram dificuldades no processo de interpretar a lei e na mudança de paradigma da rotina de trabalho, a fim de adequar os novos sistemas e os sistemas legados com a legislação vigente. Como contribuição teórica, o artigo apresenta uma proposta baseada em padrões de privacidade para apoiar a definição de requisitos alinhados com a LGPD. A proposta foi avaliada no contexto do sistema Nísia, que é um aplicativo móvel implementado pela organização.

O artigo está dividido nas seguintes seções. A Seção 2 apresenta o background de referencial teórico sobre requisitos de privacidade e Lei Geral de Proteção de Dados. A Seção 3 descreve a metodologia utilizada na pesquisa, apresenta o contexto do estudo de caso, assim como descreve as etapas de coleta e análise de dados. A Seção 4 descreve os resultados obtidos no estudo de caso. A Seção 5 apresenta uma proposta de padrões de privacidade para auxiliar analistas na especificação dos requisitos de privacidade em conformidade com a LGPD. Finalmente, na Seção 6 são apresentadas as conclusões, limitações da pesquisa e trabalhos futuros.

2 Background

2.1 Requisitos de Privacidade

Privacidade é um conceito amplamente investigado em diferentes áreas, tais como, direito, filosofia e sociologia. Recentemente, privacidade tem sido um tema de crescente interesse da comunidade de engenharia de requisitos. Requisitos de privacidade são difíceis de quantificar e especificar com precisão [5,9]. Martin e Kung [10] seguem o mesmo raciocínio afirmando que engenheiros de software estão habituados a pensar em termos de modelos de dados e arquiteturas. Todavia, eles se sentem perdidos para traduzir questões regulatórias nas suas atividades de desenvolvimento.

Segundo Kalloniatis [11], privacidade é o direito em determinar quando, como e em que condições é permitido compartilhar informações pessoais e transmitir tais informações para terceiros. A partir de um mapeamento sistemático conduzido por Anthonysamy et al. [4], requisitos de privacidade podem ser classificados em quatro categorias de acordo com a compreensão sobre a natureza e a perspectiva do usuário, são elas: conformidade, controle de acesso, verificação e usabilidade. A seguir descrevemos cada categoria proposta por [4].

A privacidade na perspectiva de **conformidade** opera com base em requisitos de privacidade decorrentes da legislação de proteção de dados, tendo como foco a obtenção e análise de requisitos necessários para desenvolver sistemas. O foco dessa visão é a obtenção e análise de requisitos necessários para desenvolver sistemas de software. Esta perspectiva faz o uso de referenciais teóricos fornecidos por juristas e estruturas de padrões de segurança e privacidade para eliciar requisitos de privacidade. A privacidade na perspectiva do **controle de acesso** é conhecida por ser uma tarefa difícil e problemática para usuários em diversas áreas de segurança, como autenticação, autorização, etc. Esta categoria foca na definição de mecanismos de controle de acesso em relação às informações divulgadas ao usuário. A privacidade na perspectiva de **verificação e correção** de sistemas de software tem como objetivo a aplicação de métodos formais para verificação de requisitos de segurança e privacidade a fim de aumentar a confiabilidade dos sistemas de software. A privacidade sob a perspectiva de **usabilidade** concentra na avaliação de comportamentos, necessidades e motivações dos usuários através de técnicas de observação e análise de problemas de usabilidade para aplicar em soluções que garantam a privacidade dos usuários. Esta perspectiva cobre um amplo espectro que inclui estudos centrados nos usuários sobre suas percepções de privacidade, violações de privacidade nas mídias sociais e melhoria da conscientização e comportamentos dos usuários.

Hadar e colegas [6] reforçam a necessidade de abordagens sistemáticas para especificar requisitos de privacidade pois muitos profissionais da área não possuem conhecimento e compreensão suficiente sobre conceitos de privacidade. Nesta mesma direção, Canedo et al. [12] consideram que engenheiros de software possuem pouco conhecimento sobre como garantir que sistemas estejam em conformidade com legislações que visam a proteção de dados de usuários. Com o objetivo de oferecer uma visão ampla sobre requisitos de privacidade, Peixoto et al. [23] propuseram um modelo conceitual e um catálogo de conceitos relacionados a requisitos de privacidade. O modelo

conceitual apresenta diversos mecanismos de privacidade que podem ser úteis para guiar o desenvolvimento de sistemas de software aderentes a requisitos de privacidade. Na mesma direção, Gharib et al. [7] desenvolveram uma ampla ontologia para modelar requisitos de privacidade, tais requisitos são refinados nos conceitos: confidencialidade, anonimização, pseudonimização, inobservidade, notificação, transparência, responsabilização.

2.2 Lei Geral de Proteção de Dados (LGPD)

A LGPD entrou em vigor no dia 18 de setembro de 2020 mantendo a linha da GDPR, possibilitando as relações entre Brasil e a União Europeia com segurança de dados equivalentes. A LGPD serve de eixo para o sistema normativo brasileiro de proteção de dados pessoais [13]. A lei determina o que pode e não pode ser feito em relação à coleta de dados no país, prevendo punições para as empresas que desrespeitarem os seus dispositivos. A LGPD regula as operações de tratamento de dados pessoais realizadas por agentes públicos e privados, ou seja, regula o acesso, coleta, armazenamento, processamento e compartilhamento de dados pessoais.

A LGPD possui 65 artigos distribuídos em definições, conceitos, princípios, sanções e requisitos para tratamento de dados. Dentre os principais conceitos destacamos os tipos de dados: **dado pessoal**, que é a informação relacionada a pessoa natural identificada ou identificável; **dado pessoal sensível**, que trata sobre origem racial, religião, saúde e opção sexual; **dado anonimizado**, que se refere ao dado relativo ao titular que não possa ser identificável; e **dado pseudonimização**, que é o tratamento para perder associação ou link direto ou indireto do indivíduo, mas com possibilidade de recuperar a origem.

Considerando que a LGPD entrou em vigor recentemente, empresas de diferentes setores e órgãos públicos ainda estão enfrentando desafios para adequarem seus sistemas de software em conformidade com a legislação vigente. Garantir a conformidade legal visa evitar que sanções administrativas sejam aplicadas pela autoridade nacional de proteção de dados. As infrações à LGPD vão desde advertência até a imposição de sanções de natureza pecuniária que pode chegar a 2% do faturamento da empresa, limitada a R$50 milhões por infração.

3 Método de Pesquisa

Este artigo tem como objetivo investigar as seguintes questões de pesquisa:

QP1. Quais são as percepções de analistas de requisitos em relação à privacidade e proteção de dados?

QP2. Como auxiliar analistas de requisitos na especificação de requisitos de privacidade em conformidade com a LGPD?

Para responder as questões de pesquisa, conduzimos um estudo de caso em uma organização que visa adotar novas práticas de engenharia de requisitos alinhadas com a LGPD. O estudo de caso seguiu as recomendações de Merrian [14] e utilizou teoria fundamentada nos dados [17]. O propósito do estudo de caso foi conduzir uma pesquisa

exploratória e descritiva, pois tem como características principais investigar como analistas de requisitos entendem a privacidade de dados pessoais e quais são suas preocupações e desafios enfrentados durante a especificação de tais requisitos. A partir das percepções dos analistas de requisitos, nossa pesquisa visa propor uma abordagem para apoiar a especificação de requisitos de privacidade em conformidade com a LGPD.

3.1 Contexto do Estudo de Caso

O estudo de caso foi conduzido em uma organização do poder judiciário estadual. Ao longo dos anos, a organização tem buscado inovar na área de TI. Ela tem participado ativamente na implantação do Processo Judicial Eletrônico (PJe). O objetivo principal é manter um sistema eletrônico capaz de permitir a prática de atos processuais em todos os ramos do Judiciário (Federal, Estadual e do Trabalho). Considerando a recente necessidade de adequação à LGPD, identificamos a oportunidade de contribuir com a melhoria do processo de requisitos da organização. É importante ressaltar que o segundo autor desse artigo desempenhou durante muitos anos a função de analista de requisitos e hoje atua como gerente de projetos na organização estudada. Dessa forma, este artigo visa investigar um problema real enfrentado pela organização.

Para apoiar a análise do estudo de caso, escolhemos o sistema Nísia [18] que foi implementado pela equipe de TI da organização. O Nísia é um aplicativo desenvolvido com o objetivo de possibilitar melhor acesso à informação de processos de medida protetiva. Com o aplicativo, a mulher ofendida pode acompanhar o andamento do processo pelo seu telefone celular sem precisar se deslocar até o órgão julgador onde tramita o processo. Neste contexto, existe uma preocupação predominante de se preservar as mulheres, que são vítimas de violência doméstica independente de terem ou não processos tramitando no judiciário. O aplicativo pode ser acessado pela própria vítima de violência ou qualquer pessoa que sinta o desejo de ajudar uma mulher em situação de violência. Considerando o perfil dos usuários (i.e., mulheres que sofrem violência) e a natureza de dados sensíveis acessados pelo aplicativo Nísia, requisitos de privacidade são aspectos críticos que o sistema precisa satisfazer.

3.2 Coleta de Dados

Para realizar a coleta de dados, conduzimos entrevistas semiestruturadas com 5 analistas de requisitos da organização. Todos os participantes possuem mais de dez anos de experiência e também acumulam cargos de gestão nas suas equipes, tais como: coordenação, chefia, direção e gerência. A Tabela 1 apresenta o perfil dos entrevistados.

As entrevistas ocorreram no período de outubro a dezembro de 2020 e utilizamos a ferramenta Cisco Webex de videoconferência. O protocolo de entrevista possui 27 questões e está disponível em: https://tinyurl.com/1v9qlngf. Todas as entrevistas foram gravadas e resultaram em cerca de seis horas e trinta minutos de gravação. Com os dados coletados nas entrevistas, foi possível investigar o ponto de vista dos analistas de requisitos buscando compreender suas percepções durante a especificação de requisitos de privacidade e entender como a organização está trabalhando seus processos internos para garantir conformidade com a LGPD.

Tabela 1. Perfil dos entrevistados

ID	Experiência profissional	Função
E1	15 anos	Chefe do Núcleo de Gestão de Processos e Serviços de TI e Analista de requisitos
E2	18 anos	Gerente de arquitetura de negócios e Engenheiro de Software
E3	20 anos	Analista de requisitos e Chefe do Núcleo de Gestão de Segurança da Informação
E4	13 anos	Diretor de Sistemas e Analista de requisitos
E5	20 anos	Gerente de Projetos e Analista de requisitos

3.3 Análise e Síntese de Dados

Durante a fase de análise, adotamos a abordagem de Teoria Fundamentada nos Dados (TFD), do inglês *Grounded Theory*, que envolveu as fases de codificação aberta, codificação axial e codificação seletiva. A TFD tem como objetivo criar uma teoria a partir dos dados coletados e analisados sistematicamente com o processo central de codificação dos dados. Segundo Strauss e Corbin [17], durante a codificação são identificados conceitos (ou códigos) e categorias. Um conceito dá nome a um fenômeno de interesse para o pesquisador. Categorias são agrupamentos de conceitos unidos em um grau de abstração mais alto. O produto final da pesquisa na teoria fundamentada é uma série de conceitos fundamentados e integrados em torno de uma categoria ou questão central para formar um arcabouço teórico que explique como e porque as pessoas reagem a determinados acontecimentos, desafios ou problemáticas.

O processo de análise dos dados foi realizado da seguinte forma. Inicialmente utilizamos a codificação aberta. Nesse momento as entrevistas foram lidas e analisadas por um dos autores, realizando as codificações individuais com anotações, comentários e observações nas margens dos documentos transcritos. Este procedimento foi realizado nas cinco entrevistas, com o objetivo de identificar dados de potencial relevância, com semelhanças e diferenças para descrever o fenômeno em estudo e responder as questões de pesquisa. Nessa etapa, várias interações de comparações foram realizadas para a seleção de códigos que indicavam relatos representativos em citações de cada entrevista. Na codificação aberta, a comparação e os questionamentos são dois procedimentos analíticos básicos que propiciam mais precisão e especificidade às características fundamentais aos conceitos [17]. Na Figura 1, apresentamos o exemplo de um trecho de entrevista, com seu respectivo código.

Durante o processo de codificação axial, que consiste em aprimorar e diferenciar as categorias resultantes da codificação aberta, criamos os relacionamentos entre os códigos através das categorias onde elaboramos temas de ordem superior. Segundo Cruzes e Dyba [16], categorias são conceitos unificadores recorrentes ou declarações sobre o assunto investigado, com o propósito de caracterizar evidências de estudos individuais em percepções mais gerais de um conjunto de dados.

Fig. 1. Evidência da entrevista, ponto chave e código

[E4] – "Acho que o produto do trabalho desse comitê que está atuando para implantar a LGPD aqui no tribunal, vai ajudar muito a gente nesse sentido, tenho a expectativa que a gente tenha assim um cheque list de coisas que a gente vá precisar implementar para garantir que os sistemas e que isso vá servir de base line para entregar os sistemas conforme a lei prevê."

Ponto chave: Operacionalizar a interpretação da lei

Código: Operacionalizar a interpretação da lei -> Falta de processo de conformidade

Finalmente, a codificação seletiva é a fase de refinamento da codificação axial em um nível superior de abstração, onde o objetivo é integrar e sintetizar categorias em um nível mais abstrato. Segundo Strauss e Corbin [17], o fenômeno central é o coração do processo de integração. Nessa etapa, elaboramos a categoria central *especificação de requisitos em conformidade com a LGPD*, em torno da qual as outras categorias foram desenvolvidas e integradas. Na síntese dos dados, foi realizada uma classificação final das categorias, considerando como critério de definição das categorias, o grau de relevância em relação aos aspectos de privacidade de dados na especificação de requisitos em conformidade legal. O processo de codificação iniciou com 48 páginas de dados brutos e foram identificados 25 códigos. Finalmente, os códigos foram agrupados em 5 categorias detalhadas na próxima seção.

4 Resultados das Entrevistas

Nesta seção, apresentamos os resultados obtidos a partir das entrevistas realizadas. A seguir discutimos os principais achados e trechos de falas dos entrevistados dentro de cinco categorias identificadas.

4.1 Conceitos de Privacidade

Esta categoria diz respeito a limitação de conhecimento sobre princípios e conceitos de privacidade e proteção de dados. É por meio do conhecimento apropriado sobre a legislação vigente e como ela pode ser operacionalizada em requisitos de privacidade que os sistemas novos e legados estarão em conformidade com a LGPD. Identificamos nos relatos dos entrevistados, que a falta de entendimento conceitual sobre privacidade de dados, trás como consequências a fragilidade de especificar requisitos de privacidade, assim como a falta de maturidade na operacionalidade das regras legais impacta o correto desenvolvimento de novos sistemas. A seguir apresentamos evidências encontradas nas entrevistas:

[E1] "Eles (equipe de TI) têm total desconhecimento, até porque ***o requisito de segurança da informação que está ligado a LGPD como requisito não funcional, ele nunca foi uma prioridade*** *no desenvolvimento de sistemas."*

[E5] "Eu acho que a minha equipe entende o que é divulgado na mídia, mas ***não tem o entendimento profundo sobre esta questão. É o que tá no dia a dia, na cultura ou mesmo por ética e valor da própria pessoa.****"*

Diante dessa preocupação, os entrevistados reforçaram que o primeiro passo necessário para garantir um conhecimento amplo sobre privacidade e proteção de dados envolve investimento em capacitação e conscientização sobre o tema. Isto pode ser evidenciado nos seguintes trechos:

[E2] "Quanto aos métodos ou modelos, penso que devemos trabalhar em cima das ***capacitações das pessoas, para elas entenderem o que são essas preocupações de privacidade*** *e elas embutem isso nas especificações que eles vão fazer."*

[E3] "Acho que existe um nível de preocupação, ***acho que esse conhecimento não está zerado, mas acho que é algo que precisa ser amadurecido diante dos requisitos atuais.*** *A realidade de agora exige uma preocupação mais reforçada do que vinha se tendo. Acho que nossa equipe precisa-se amadurecer para os requisitos de agora. O primeiro passo para esse amadurecimento vem com o* ***trabalho de conscientização****, que já iniciamos com cursos de capacitação."*

[E5] "Eles (equipe de TI) não fizeram cursos de proteção de dados e não foram capacitados formalmente para isso. (...) a quantidade de sistemas de informações disponibilizado para o público aumenta exponencialmente, então a gente precisa ter uma ***capacitação atualizada dessas questões de dados pessoais****."*

4.2 Processo de Conformidade

Esta categoria envolve o modo sistemático como a organização deseja operacionalizar a adequação dos seus processos internos e sistemas de software à legislação vigente. Verificamos que a principal necessidade destacada pelos entrevistados é a operacionalização da interpretação da lei, isto é visto como um desejo unânime entre os entrevistados. A necessidade de garantir a conformidade com a legislação está diretamente ligada a ausência de um processo, modelo ou método que auxilie na especificação de requisitos de privacidade em conformidade com a LGPD. Estes aspectos podem ser evidenciados nos seguintes trechos de entrevistas:

[E1] "Estou imaginando um ***comitê que tenha pessoas da informática e assessoria jurídica****, que traga propostas para traduzir em forma de* ***template****, até porque esse tipo de informação se repete...que esse comitê venha operacionalizar a interpretação da lei, cabendo a essa pessoa de TI ajudar nessa operacionalização e disseminar conhecimento nas equipes de TI."*

[E4] "Acho que o produto do trabalho ***desse comitê, que está atuando para implantar a LGPD*** *aqui, vai ajudar muito a gente nesse sentido, tenho a expectativa que a gente tenha* ***um checklist de coisas que a gente vá precisar implementar para garantir que os sistemas*** *estejam em conformidade e que isso vá servir de baseline para entregar os sistemas conforme a lei prevê."*

[E5] "Seria um ***template que operacionalizasse essa especificação dos requisitos*** *de privacidade com campos obrigatórios, acho isso iria ajudar muito."*

4.3 Obstáculos na Conformidade

Esta categoria explora a forma como a organização encara os obstáculos para alinhar os seus sistemas, bases de dados, e a própria mentalidade das pessoas envolvidas em

relação aos aspectos de privacidade em conformidade legal. Observamos nos relatos dos entrevistados que as maiores dificuldades são evidenciadas como a complexidade na aplicabilidade da LGPD, onde a principal preocupação dos analistas é satisfazer as regras de negócios. Além disso, os entrevistados relataram que a atual cultura organizacional é considerada um obstáculo. Estes achados podem ser evidenciados nos seguintes trechos das entrevistas:

*[E2] "**Não existe essa preocupação com proteção e privacidade de dados, a preocupação é pela regra de negócio**. A preocupação é para deixar o sistema rodando em produção."*

*[E1] "**Não existe essa cultura de especificar de forma explícita os requisitos de privacidade**, (...) vai ser um grande desafio a LGPD porque de fato a coisa está muito embrionária."*

*[E2] "A maior dificuldade que vamos encontrar está na **cultura da nossa organização**, (...) a nossa instituição a cada dois anos troca de gestão, quando muda a gestão muda as pessoas, mas existe um conjunto de comportamentos e culturas que permanecem e acho que **essa é a maior dificuldade que é uma cultura** independente das pessoas."*

*[E3] "Me parece que a alta gestão já tem um nível de sensibilidade para isto. O que me preocupa mais não é a alta gestão, mas a operação mesmo**, a gente descer para os níveis mais táticos e operacionais**."*

4.4 *Tradeoff* entre Privacidade e Transparência

Esta categoria refere-se ao modo como a organização sofre influência das leis internas e externas vigentes e o impacto das novas legislações nos seus sistemas e serviços prestados. Observamos que existe um verdadeiro dilema entre os entrevistados, na forma como tratar os diversos tipos de dados conforme a lei e a necessidade, ou melhor, alinhar os conceitos de privacidade com outras leis vigentes, como a Lei de Acesso a Informação (LAI). Este é um desafio enfrentado por organizações públicas em geral. A equipe de TI precisa diferenciar como disponibilizar informações que são privadas daquelas que precisam ser públicas. Isso reflete um *tradeoff* entre privacidade e transparência e que pode ser confirmado nos seguintes trechos:

*[E3] "O desafio que é o esclarecimento dos aspectos da lei geral de proteção de dados no âmbito do judiciário, que mostre a consonância da LGPD com as leis que já regem nosso funcionamento (códigos de processos, LAI), é um desafio grande a gente **lidar com lei a de acesso à informação e a lei de privacidade de dados, que é transparência x privacidade**."*

*[E4] "Eu acho que devemos analisar caso a caso, e acho que sim, que pode surgir situações de conflito, a depender da informação que o cidadão deseja ter e isso pode entrar em conflito com a LGPD e gerar uma situação delicada**. Eu acredito que na maioria dos casos seja possível haver uma conciliação.** Essas informações requisitadas com base na LAI, geralmente não tem um propósito de requisitar dados pessoais, geralmente chega solicitação para finalidade de pesquisas acadêmicas ou para matéria jornalística."*

[E5] "Se formos pecar por excesso, vamos colocar tudo como segredo de justiça, aí você pode estar prejudicando a população onde o processo tem que ser público(...) então ***esse limite entre o que tem que ser público e sigiloso não está bem definido****,* ***e esse limite que muitas vezes não é dado pela legislação****."*

Por outro lado, vimos que sistemas que tratam de casos em segredo de justiça já tem as caraterísticas inerentes de privacidade devido a relevância social, a situação delicada numa eventual exposição desses dados e a exigência de lei específica. Isso pode ser reforçado no seguinte trecho:

[E4] "São mulheres vítimas de violência doméstica. E como são pessoas que estão em situação de vulnerabilidade, (...) a gente sabe que ***se essas informações de alguma forma vazarem, as vítimas podem sofrer agressão*** *e até perder a vida. Então a gente se preocupa muito com isso."*

4.5 Rotina de Trabalho

Esta categoria refere-se ao modo como as equipes de TI da organização realizam seu trabalho, envolvendo suas competências e atividades do dia a dia. Segundo relatos dos entrevistados, muitas vezes os aspectos de privacidade são tratados de maneira intuitiva pelas equipes envolvidas. Como não há uma estratégia ou processo bem definido, requisitos de privacidade são abordados de maneira *ad hoc*.

[E3] "A privacidade é tocada em soluções internas muito mais pelo feeling, e quando a gente tem outra legislação específica, por exemplo: dados sobre criança e adolescente, já uma questão que já tratamos e rebate no tema de privacidade… ***essas questões de privacidade às vezes são tratadas por intuição ou ad hoc.****"*

*[E5] "****Não tem processo formal, não tem ferramenta, método ou modelo que contemplem os aspectos de privacidade. Então vai mais pelo feeling do engenheiro de requisitos****, inclusive ele pode esquecer de contemplar os aspectos de privacidade, que isso já aconteceu, usuários tiveram acessos a fluxos do processo que não poderia ver."*

Um ponto de fragilidade levantado pelos entrevistados é a limitação de recursos de pessoal. Diante disso, ficou claro que a prioridade é entregar o produto com agilidade, devido ao grande volume de sistemas e novas demandas. Os projetos possuem poucas pessoas, e nem todas que estão disponíveis são capacitadas. Esta questão pode ser evidenciada nos seguintes trechos das entrevistas:

*[E4] "****A cabeça de quem é de TI é meio cartesiana, eles querem modelos****, parametrizar, digamos assim que tem que ser parametrizada. (...) temos um volume grande de coisas para fazer, as demandas são muitas e precisamos de algo para dar vazão, que possa viabilizar a implantação dessas coisas mais produtiva."*

*[E2] "****A equipe até tem o conhecimento, mas devido a celeridade da entrega dos sistemas o tratamento não é o adequado****. (...) Nós temos uma equipe limitada de recursos, de pessoas capacitadas para fazer esse tipo de levantamento de requisitos e são muitas coisas para fazer, então* ***eles vão fazer rápido para liberar logo****."*

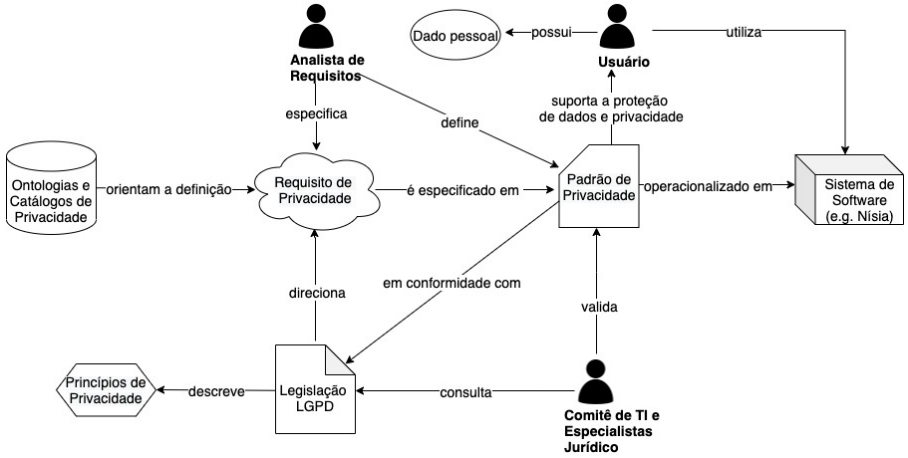
[E4] "Para mim ***a dificuldade é de conciliar a mão de obra*** *mesmo, em função de outras demandas que temos. (...) para mim o trabalho maior será em fazer a adaptação desses sistemas legados, então acho que esse será o maior desafio."*

5 Padrões de Privacidade em conformidade com a LGPD

A partir da análise das percepções dos entrevistados, identificamos que os analistas de requisitos da organização necessitam de uma abordagem para especificar requisitos de privacidade que seja ágil e forneça diretrizes simples em formato de *templates* ou *checklists*. Além disso, num primeiro momento, a organização precisa realizar ações de conscientização e capacitação a fim de disseminar uma cultura alinhada com valores de privacidade. Dessa forma, a abordagem deve apresentar *guidelines* claros e boas práticas para garantir seu uso de forma fácil e rápida. Considerando tais necessidades, elaboramos uma proposta baseada em padrões de privacidade para apoiar a especificação de requisitos de privacidade em conformidade com a LGPD. Nossa motivação para utilização de padrões é devido a sua ampla adoção pela comunidade de Engenharia de Software. Padrões fornecem uma estrutura simples para sistematizar e reusar conhecimento e compartilhar boas práticas [20]. Além disso, diferentes padrões de privacidade têm sido propostos por vários pesquisadores [19].

A Figura 2 apresenta uma visão geral da nossa abordagem. Consideramos que os padrões de privacidade serão definidos por analistas de requisitos e validados por um comitê multidisciplinar com profissionais de TI e especialistas jurídicos. Para garantir a disseminação de uma visão compartilhada sobre conceitos de privacidade e proteção de dados, adotamos ontologias [7] e catálogos [23] como base de conhecimento na área. Tais bases de conhecimento tem como objetivo orientar a definição de requisitos que serão especificados no formato de padrões de privacidade. O objetivo do padrão de privacidade é definir de forma clara e simples como requisitos de privacidade em conformidade com a LGPD serão operacionalizados e implementados nos sistemas.

Fig. 2. Visão Geral da Proposta de Padrões de Privacidade



A nossa proposta de padrões de privacidade foi inspirada nos trabalhos [15, 20, 21, 22]. A Tabela 2 apresenta um padrão de privacidade composto por elementos que auxiliam o entendimento e operacionalização da LGPD. O padrão foi definido no contexto do aplicativo Nísia que já está em operação e disponível para o público. A organização

pretende usar este sistema como prova de conceito a fim de melhorar suas práticas para especificação de requisitos de privacidade. Dessa forma, iremos elaborar um catálogo de padrões de privacidade para guiar as futuras evoluções do sistema e garantir sua conformidade com a LGPD.

Tabela 2. Padrão de Privacidade

ID e Nome do Padrão	[PP01] Compartilhamento de Dados
Problema	Para acesso ao aplicativo Nísia, os dados fornecidos para o cadastro do(a) usuário(a) (i.e. titular do dado) poderão ser compartilhados com outros órgãos públicos ou particulares envolvidos na demanda.
Conformidade Legal	Lei 13.709 – LGPD Art. 26º; Art. 6º, inciso I, III, V e VII
Descrição legal	Antes de iniciar a coleta dos dados de CPF e e-mail do(a) titular, o agente (i.e. comitê gestor dos dados) deve se certificar previamente que a finalidade da operação esteja registrada de forma clara e explícita. Sempre respeitando os limites legais, contratuais da finalidade, propósitos especificados e informados ao titular dos dados, e dispensando o consentimento por se tratar de execução de políticas públicas devidamente previstas em lei.
Objetivo de Privacidade	Atender os princípios da finalidade, necessidade, qualidade dos dados e segurança.
Ativos	Dados da mulher vítima de violência sob medida protetiva, movimentações realizadas no processo, órgão julgador e tipo do processo (físico ou eletrônico).
Vulnerabilidades	Vazamentos de informações sobre o andamento do processo
Solução	Coletar os dados necessários para a finalidade específica de cadastro e utilizar a técnica de pseudonimização para evitar associação entre o dado e o titular, mas com a possibilidade de reversão e identificação da origem.
Consequências	Evitar que dados da mulher vítima de violência sob medida protetiva sejam acessados de forma indevida. Mostrar ao usuário(a) (i.e. titular do dado) que o aplicativo trata seus dados com responsabilidade a fim de aumentar sua confiança.

6 Conclusões, Limitações e Trabalhos Futuros

Este artigo apresentou um estudo de caso com o objetivo de investigar a perspectiva de analistas de requisitos sobre privacidade e proteção de dados. Trabalhos semelhantes que também buscavam entender a visão de desenvolvedores incluem os estudos [8] e [12]. Diferente desses artigos, nossa pesquisa realizou um estudo de caso com analistas de uma única organização para entender o problema com maior profundidade. Os resultados do estudo de caso revelaram que os analistas da organização estudada consideram que é necessário investir em capacitação e comunicação interna para disseminar aspectos de privacidade em conformidade com a LGPD. Outra percepção que teve

destaque foi em relação a rotina de trabalho. Os entrevistados relataram que possuem equipes com pessoal bastante limitado para atender novas demandas. Eles reforçaram que já existe um sentimento sobre a relevância da privacidade presente nas equipes, pois alguns sistemas já exigiam que tais requisitos fossem satisfeitos antes da lei entrar em vigor. Eles compartilharam a dificuldade de interpretar e operacionalizar a LGPD no contexto dos sistemas e serviços prestados. Como forma para tratar tais desafios, os entrevistados mencionaram a necessidade de uma abordagem ágil e simples para especificar requisitos de privacidade. A partir dos insights das entrevistas, elaboramos uma abordagem baseada em padrões de privacidade. Como demonstração da proposta, definimos um padrão de privacidade específico para o contexto do sistema Nísia.

O artigo apresenta algumas limitações. A interpretação e síntese dos dados foi realizada por ambos autores para minimizar o vié. Como realizamos entrevistas semiestruturadas com analistas de requisitos, os dados coletados são referentes as opiniões pessoais desses participantes. Como forma de atacar essa limitação, buscamos selecionar analistas de diferentes equipes, com mais de 10 anos de experiência na área e que atualmente assumiram cargos gerenciais na organização. Como o estudo foi realizado com apenas cinco analistas de uma única organização, não podemos afirmar que os resultados do estudo possam ser amplamente generalizados. Assim, precisaríamos realizar estudos complementares para entender o contexto de diferentes organizações, como empresas privadas, por exemplo. Apesar dessas limitações, nossos resultados apresentam evidências qualitativas e insights ricos para avançar o entendimento sobre requisitos de privacidade.

Como trabalhos futuros, pretendemos explorar com mais profundidade os dados obtidos nas entrevistas e refinar a análise das categorias já definidas. Iremos elaborar um catálogo de padrões de privacidade e aplicar nos sistemas desenvolvidos pela organização. Além disso, vamos propor práticas ágeis para apoiar o processo de elicitação, especificação e validação de requisitos de privacidade. Em seguida, iremos avaliar os artefatos propostos com analistas de requisitos da organização estudada assim como de outras organizações. Em síntese, nossa agenda de pesquisa envolve a realização de pesquisas empíricas para investigar como as organizações estão evoluindo seus processos de engenharia de requisitos para garantir que os sistemas de software estejam em conformidade com a LGPD.

Referências

1. https://securityinformationnews.com/2019/09/07/ministerio-publico-acusa-vivo-por-vender-indevidamente-dados-de-73-milhoes-de-usuarios/, último acesso em 08/02/2021.
2. https://tinyurl.com/maiorvazamentodedados, último acesso em 08/02/2021.
3. Kalloniatis, C.: Incorporating privacy in the design of cloud-based systems: a conceptual meta-model. Information & Computer Security. vol. 25, No. 5, (2017).
4. Anthonysamy, P., Rashid A., Chitchyan, R.: Privacy Requirements: Present & Future. IEEE/ACM 39th International Conference on Software Engineering: Software Engineering in Society Track, (2017).

5. Ayala-Rivera, V., e Pasquale, L.: “The Grace Period Has Ended”: An Approach to Operationalize GDPR Requirements. IEEE 26th International Requirements Engineering Conference. 2018.
6. Hadar, I., Hasson, T., Ayalon, O., Toch, E., Birnhack, M., Sherman, S., & Balissa, A.: Privacy by designers: software developers’ privacy mindset. Empirical Software Engineering, (2018).
7. Gharib, M., Mylopoulos J., Giorgini P. A core ontology for privacy requirements engineering. Research Challenges in Information Science. RCIS 2020. Lecture Notes in Business Information Processing, vol 385. Springer, (2020).
8. Peixoto M. et al.: On Understanding How Developers Perceive and Interpret Privacy Requirements Research Preview. International Working Conference on Requirements Engineering: Foundation for Software Quality. REFSQ 2020. (2020).
9. Webster, I., Ivanova, V.: Reusable Knowledge for Achieving Privacy: A Canadian Health Information Technologies Perspective. Workshop em Engenharia de Requisitos. WER2005. (2005).
10. Martin, Y. S., Kung, A.: Methods and Tools for GDPR Compliance through Privacy and Data Protection Engineering, IEEE European Symposium on Security and Privacy Workshops, (2018).
11. Kalloniatis, C.; Kavakli, E.; Gritzalis, S.: Addressing privacy requirements in system design: the PriS method. Requirements Engineering. v.13, pp. 241-255, (2008).
12. Canedo, E. D., Calazans, A. T. S., Masson, E. T. S., Costa, P. H. T., Lima, F.: Perceptions of ITC Practitioners Regarding Software Privacy. Entropy, (2020).
13. Maldonado, V. N., Blum, R. O.: LGPD: Lei Geral de Proteção de Dados Comentada, Thompson Reuters Brasil Conteúdo e Tecnologia Ltda, (2019).
14. Merriam, Sharan B.: Qualitative Research: a guide to design and implementation, (2009).
15. Xuan, X., Wang Y., Li, S.: Privacy Requirements Patterns for mobile Operating Systems, IEEE 4th International Workshop on Requirements Patterns (RePa), (2014).
16. Cruzes, D. e Dyba, T.: Recommended Steps for Thematic Synthesis in Software Engineering. International Symposium on Empirical Software Engineering and Measurement, (2011).
17. Strauss, A. e Corbin J.: Basics of Qualitative Research: Grounded Theory Procedures and Techniques. London, 2 edição, Sage Publications (1998).
18. Aplicativo Nísia, https://www.cnj.jus.br/aplicativo-tem-novas-funcionalidades-e-orienta-mulher-vitima-de-violencia-em-pernambuco/, último acesso em 29/03/2021.
19. Lenhard, J., Fritsch, L. e Herold, S.: A Literature Study on Privacy Patterns Research, 43rd Euromicro Conference on Software Engineering and Advanced Applications, SEAA, (2017).
20. Franch, X., Palomares, C., Quer, C., Renault, S., Lazzer, F.: A Metamodel for Software Requirements Patterns, International Working Conference on Requirements Engineering: Foundation for Software Quality. REFSQ 2010. (2010).
21. Salini, P. e Kanmani, S.: A Knowledge-Oriented Approach to Security Requirements Engineering for E-Voting System, International Journal of Computer Applications, (2012).
22. https://privacypatterns.eu/ último acesso em 31/03/2021.
23. Peixoto, M., Silva, C. Maia, H. Araújo, J.: Towards a Catalog of Privacy Related Concepts. Joint Proceedings of REFSQ 2020, Workshops, Doctoral Symposium, Live Studies Track. (2020).